

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004 年 4 月 29 日 (29.04.2004)

PCT

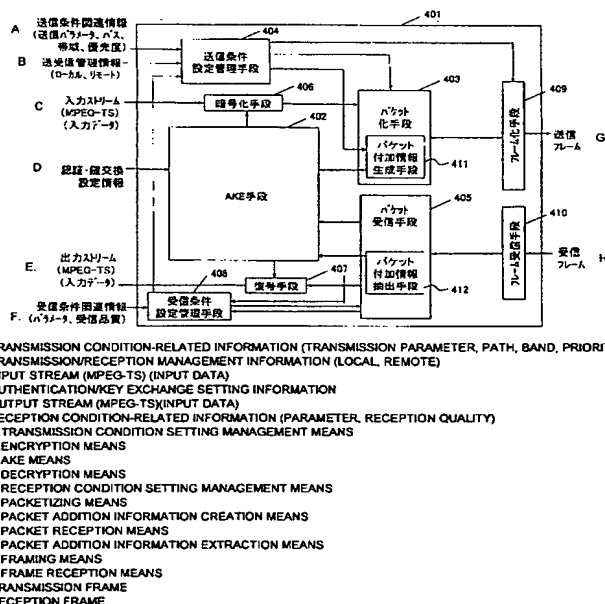
(10) 国際公開番号
WO 2004/036840 A1

- (51) 国際特許分類⁷: H04L 12/56, 9/00 (71) 出願人 (米国を除く全ての指定国について): 松下電
器産業株式会社 (MATSUSHITA ELECTRIC INDUS-
(21) 国際出願番号: PCT/JP2003/013218 TRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市
大字門真 1 0 0 6 番地 Osaka (JP).
(22) 国際出願日: 2003 年 10 月 15 日 (15.10.2003)
(25) 国際出願の言語: 日本語 (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 森岡 芳宏
(26) 国際公開の言語: 日本語 (MORIOKA, Yoshihiro) [JP/JP]; 〒639-0261 奈良県
香芝市 尼寺三丁目 4 7 6-5 1 Nara (JP). 綾木 靖
(30) 優先権データ: (AYAKI, Yasushi) [JP/JP]; 〒572-0037 大阪府 寝屋川
市 葛原新町 1 3-1-2 0 6 Osaka (JP). 三谷 浩 (MI-
特願 2002-302924 TANI, Hiroshi) [JP/JP]; 〒575-0044 大阪府 四條畷市 二
丁通町 5-1 4 Osaka (JP). 臼木 直司 (USUKI, Naoshi)
特願 2002-340582 [JP/JP]; 〒614-8331 京都府 八幡市 橋本意足 2 6-1 2
2002 年 10 月 17 日 (17.10.2002) JP
2002 年 11 月 25 日 (25.11.2002) JP
Kyoto (JP).

[続葉有]

(54) Title: PACKET TRANSMISSION/RECEPTION DEVICE

(54) 発明の名称: パケット送受信装置



(57) Abstract: A packet transmission/reception device includes: authentication/key exchange means; encryption means for creating encrypted transmission data; transmission condition setting management means for creating transmission condition setting information for setting a transmission condition of a transmission packet; packetizing means for creating a transmission packet by using the encrypted transmission data; reception condition setting management means for creating reception condition setting information for setting a reception condition of a reception packet; packet reception means for receiving the reception packet; and decryption means for decrypting the reception data by using a decryption key.

(57) 要約: パケット送受信装置であって、認証・鍵交換手段と、暗号化送信データを生成する暗号化手段と、送信パケットの送信条件を設定する送信条件設定情報を生成する送信条件設定管理手段と、暗号化送信

[続葉有]



(74) 代理人: 山本 秀策, 外(YAMAMOTO, Shusaku et al.);
〒540-6015 大阪府 大阪市中央区 城見一丁目 2 番
27号クリスタルタワー 15 階 Osaka (JP).

(81) 指定国 (国内): CN, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY,
CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC,
NL, PT, RO, SE, SI, SK, TR).

添付公開書類:

— 国際調査報告書

— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

パケット送受信装置

5 技術分野

本発明は、パケット送受信装置に関する。より詳細には、本発明は、暗号化されたデータ（例えば、AVデータ）を用いてパケットを生成し、生成したパケットを、IEEE 802.3規格などに準拠するイーサネット（R）（有線LAN）、または、IEEE 802.11規格などに準拠する無線LANなどを用いて、送信および受信するパケット送受信装置に関する。

背景技術

従来、一般家庭においても、IEEE 1394規格を用いてIEC 61883-4で規定された方式に基づいて、MPEG-TSを暗号化して伝送することが行われている。MPEG-TSなどのAVデータを暗号化して伝送する方式の一例としては、DTCP (Digital Transmission Content Protection) 方式が規定されている。

DTCP方式は、IEEE 1394規格、USBなどの伝送メディア上のコンテンツ保護に関する方式である。DTCP方式は、DTLA (Digital Transmission Licencing Administrator) で規格化されている。DTCP方式は、より詳細には、例えば、<http://www.dtcp.com>、http://www.dtcp.com/data/dtcp_tut.pdf、http://www.dtcp.com/data/wp_spec.pdf、および、書籍「IEEE1394、AV機器への応用」、高田信司監修、日刊工業新聞社、「第8章、コピープロテクション」、133～149ページに説明されている。

図38は、DTCP方式を用いて、MPEG-TSを、IEEE 1394規格に準拠する伝送メディアを介して伝送すること示す模式図である。

DTCP方式では、送信装置をソース2001、受信装置をシンク2002とよび、暗号化したMPEG-TSなどのデータはソース2001からネットワーク2003を介して、シンク2002に伝送される。

図38において、ソース2001は、例えば、DVHS、DVDレコーダ、1394搭載STB (Set Top Box) または1394搭載デジタルTV (Television) であり、シンク2002は、例えば、DVHS、DVDレコーダ、1394搭載STB (Set Top Box) または1394搭載デジタルTV (Television) である。

このように、DTCP方式を用いて、IEEE 1394規格に準拠する伝送メディアを介してMPEG-TSなどのAVデータを伝送することが知られている。

しかしながら、DTCP方式をインターネットの標準プロトコルであるIPプロトコルに実装することは、今日まで知られていない。したがって、DTCP方式を用いて、AVデータを、イーサネット(R)の規格であるIEEE 802.3規格、無線LANの規格であるIEEE 802.11規格、または、その他のIPパケットを伝送可能な伝送メディアを介して伝送することはできなかった。別の言い方でいうと、従来においては、IPプロトコルを介して論理的に接続された送信装置と受信装置との間を、暗号化を用いてデータの機密性および著作権の保護を行なった状態でMPEG-TSなどのAVデータを伝送することはできなかった。

発明の開示

本発明によれば、送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、暗号化鍵および復号鍵を生成する認証・鍵交換手段と、前記

暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも1つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定するための受信条件設定情報を生成する受信条件設定管理手段と、前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、前記復号鍵を用いて前記受信データを復号する復号手段とを備える。

前記パケット化手段は、前記送信条件設定情報および前記認証・鍵交換手段に関連する認証・鍵交換関連情報の少なくとも1つを用いて、パケット付加情報を生成するパケット付加情報生成手段を含み、前記パケット化手段は、前記暗号化送信データに前記パケット付加情報を付加することによって、前記送信パケットを生成し、前記パケット受信手段は、前記送信パケットに含まれるパケット付加情報を抽出するパケット付加情報抽出手段を含む。

前記送信パケットを用いて送信フレームを生成するフレーム化手段と、受信フレームを受け取り、前記受信フレームから前記受信パケットを抽出するフレーム受信手段とをさらに備える。

前記パケット化手段にて生成された第1のパケットを一時的に蓄積する第1のキュー手段と、前記パケット化手段にて生成された第2のパケットを一時的に蓄積する第2のキュー手段と、前記送信条件設定情報に基づいて、前記第1のキュー手段に蓄積された前記第1のパケットおよび前記第2のキュー手段に蓄積され

た前記第2のケットのいずれを送信するかを制御する送信キュー制御手段と、
前記第1のキュー手段から出力された第1のケットおよび第2のキュー手段か
ら出力された第2のケットをフレーム化することによって送信フレームを生成
するフレーム化手段と、受信フレームから前記受信ケットを抽出するフレーム
5 受信手段とをさらに備える。

前記送信キュー制御手段は、前記第1のケットまたは前記第2のケットの
送信経路に関する情報と、前記第1のケットまたは前記第2のケットを送信
するのに必要な帯域幅に関する情報と、前記送信ケットの送信から到着までの
遅延に関する情報と、前記第1のケットまたは前記第2のケットの優先度に関
10 する情報とのうち少なくとも1つの情報を用いて、前記第1のキュー手段に蓄
積された前記第1のケットおよび前記第2のキュー手段に蓄積された前記第2
のケットのいずれを送信するかを制御する。

前記送信キュー制御手段は、IETF rfc2205、rfc2208、r
f c 2 2 0 9で記載されたRSVP方式、IETF rfc2210、rfc2
15 211、2212、rfc2215で記載されたIntserv方式、IETF
r f c 2 4 7 4、r f c 2 4 7 5、r f c 2 5 9 7、r f c 2 5 9 8で記載さ
れたDiffServ方式のいずれか1つの制御方式を使用する。

前記送信キュー制御手段は、前記第1のキュー手段に蓄積された前記第1のバ
ケットおよび前記第2のキュー手段に蓄積された前記第2のケットのうちのい
20 ずれかを選択して、選択したケットを優先的に出力するように前記第1のキュー
手段および前記第2のキュー手段を制御する。

前記送信キュー制御手段は、前記第2のキュー手段に蓄積された前記第1のバ
ケットの量が所定の量を超えない場合には、前記第1のキュー手段に蓄積された
前記第1のケットを優先して出力し、前記第2のキュー手段に蓄積された前記
25 第2のケットの量が所定の量を超える場合には、前記第2のキュー手段に蓄積
された前記第2のケットを優先的に出力するように前記第1のキュー手段およ

び前記第 2 のキュー手段を制御する。

前記送信キュー制御手段は、前記第 1 のキュー手段から送信される前記第 1 のパケットと前記第 2 のキュー手段から送信される前記第 2 のパケットとの間隔を平均化するように前記第 1 のキュー手段および前記第 2 のキュー手段を制御する。

5 前記送信条件設定管理手段および前記受信条件設定管理手段は、前記送信フレームの送信から到着するまでの間において前記送信パケットの送信先から受信先までの経路における最大伝送パケットサイズの検出を行ない、前記最大伝送パケットサイズ情報を用いて、前記送信条件設定情報および前記受信条件設定情報を生成する。

10 前記フレーム化手段は、前記パケット化手段にて生成された前記送信パケットに、IEEE 802.3 規格のフレームヘッダを付加する。

前記フレーム化手段は、前記パケット化手段にて生成された前記送信パケットに、IEEE 802.1Q 規格のフレームヘッダを付加する。

15 前記パケット化手段は、前記暗号化送信データを所定の大きさに変換し、IE TFでIPv4またはIPv6として規定されているIP (Internet Protocol) ヘッダを付加する。

前記パケット化手段は、IPv4ヘッダのサービスタイプフィールド、または、サービスタイプフィールド内のTOS (Type of Service) フィールドに優先パケットであることを示す情報を付加する。

20 前記パケット化手段は、IPv6ヘッダのプライオリティフィールドに優先パケットであることを示す情報を付加する。

前記パケット化手段は、第 1 のパケット化手段と、第 2 のパケット化手段とを含み、前記第 1 のパケット化手段は、前記送信条件設定情報および前記認証・鍵交換関連情報の少なくとも一つの情報を用いて前記第 1 のパケットを生成し、前記第 2 のパケット化手段は、前記送信条件設定情報と、前記認証・鍵交換関連情報と、前記暗号化送信データとの少なくとも一つの情報を用いて前記第 2 のパケ

25

ットを生成する。

前記パケット化手段は、前記暗号化送信データを所定の大きさに変換し、IETFでIPv4またはIPv6として規定されているIPヘッダを付加し、前記第1のパケット化手段はソフトウェアによって構成され、前記第2のパケット化手段はハードウェアによって構成される。

前記送信データを優先データと一般データとに分離するデータ分離手段をさらに備え、前記暗号化手段は、前記優先データを暗号化し、前記第1のパケット化手段は、前記一般データを用いて第1のパケットを生成する。

前記第1のパケット化手段は、IETF文書で規定されているデータ処理プロトコルであるRTP、RTSP、HTTP、TCP、UDP、IPのうちの少なくとも1つのヘッダを付加する。

前記第2のパケット化手段は、データにシーケンス番号を付加するか、または、IETF文書で規定されているデータ処理プロトコルであるRTP、UDP、HTTP、TCP、IPのうちの少なくとも1つのヘッダを付加する。

前記優先データは、SMPTE 259M規格で規定された非圧縮SD方式信号、または、SMPTE 292M規格で規定された非圧縮HD形式、または、IEC 61883規格で規定されたIEEE 1394によるDVまたはMPEG-TSの伝送ストリーム形式、または、DVB規格A010で規定されたDVB-ASIによるMPEG-TS形式、MPEG-PS形式、MPEG-ES形式、MPEG-PES形式の内の少なくとも一つのデータストリーム形式である。

前記第2のパケット化手段は、エラー訂正符号付加手段を含む。

前記エラー訂正符号付加手段で用いられるエラー訂正符号の方式は、リードソロモン方式、あるいはパリティ方式である。

前記暗号化鍵を示す情報は、前記フレーム化手段において前記暗号化鍵で暗号化された送信パケットを出力するより前に、前記暗号化鍵の復号情報を前記フレーム化手段から出力する。

前記暗号化鍵を示す情報は、前記暗号化鍵を用いて生成された前記暗号化送信データを含む送信パッケージが送信されるときよりも、前記送信フレームの送信から前記送信フレームに対応する受信フレームの受信までの時間より前に送信される。

- 5 前記認証・鍵交換手段は、前記パッケージ送受信装置の位置情報と、前記送信パッケージの到着先の位置情報または前記受信パッケージの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可する。

10 前記送受信管理情報は、前記パッケージ送受信装置の位置情報と、前記送信パッケージの到着先の位置情報または前記受信パッケージの送信元の位置情報との少なくとも一方を含んでいる。

前記位置情報は、例えば、地域コード、住所、郵便番号、または、経度・緯度により範囲が指定された情報である。

- 15 前記認証・鍵交換手段は、前記パッケージ送受信装置と、前記送信パッケージの到着先または前記受信パッケージの送信元との間で、前記パッケージ送受信装置から前記送信パッケージの到着先または前記受信パッケージの受信元までの片道または往復の伝播時間があらかじめ決められた制限時間より短い時間である場合に、認証を許可する。

- 20 前記認証・鍵交換手段は、前記パッケージ送受信装置と、前記送信パッケージの到着先または前記受信パッケージの送信元との間の送受信区間において無線伝送区間が存在する場合、前記無線伝送区間ではデータをスクランブルして伝送するモードであることを確認した場合に、認証を許可する。

- 25 前記認証・鍵交換手段は、前記パッケージ送受信装置と、前記送信パッケージの到着先または前記受信パッケージの送信元との間で認証を行った場合に、前記送信パッケージの到着先または前記受信パッケージの送信元に関する情報を一時的に記憶する記憶手段と、前記パッケージ送受信装置と、前記送信パッケージの到着先または前記受信パッケージの送信元とが前記あらかじめ決められた条件に合致しないために

前記認証が成立しない場合に、前記記憶手段にて記憶された情報と、前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報とを照合し、前記パケット送受信装置と前記送信パケットの到着先または前記受信パケットの送信元との間で認証を行う、照合手段とを含む。

- 5 前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報は、証明書、MACアドレスおよび生体情報の少なくとも1つを含む。

前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期間で暗号化鍵または復号鍵を更新する。

- 10 前記認証・鍵交換手段が前記復号鍵を更新するタイミングを示すタイミング情報が、前記送信パケットに付加される。

前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットのTCPポート番号、またはUDPポート番号を変化させることによって通知される。

- 15 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがHTTPを使用している場合、HTTPリクエスト毎に更新される。

また、前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがHTTPを使用している場合、一定のデータ量毎に変化される。

- 20 または、前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがRTPを使用している場合、予め決められた期間内に更新される。

前記認証・鍵交換手段におけるDTC方式のコピー制御情報は、前記送信パケットに暗号化モード情報を付加することによって伝送される。

- 25 前記優先データのデータレートが所定の値より小さくならないように、前記送信キュー制御手段は前記第1のキュー手段および前記第2のキュー手段を制御する。

前記送信キュー制御手段は、前記優先データが前記第2のキュー手段に蓄積さ

れる時間があらかじめ決めた値より常に小さくなるように、前記送信キュー制御手段は前記第 1 のキュー手段および前記第 2 のキュー手段を制御する。

前記第 2 のパケット化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、前記第 2 のパケットのパケット
5 ヘッダを生成するパケットヘッダ生成手段と、前記パケットヘッダと前記バッファから出力されるペイロードとを組み合わせるパケットを合成するパケット合成手段とを含み、前記パケットヘッダ生成手段は前記第 2 のパケットのペイロード長を指定して、前記バッファ手段に蓄積されたデータを読み出して、前記パケット合成手段に入力する。

前記第 2 のパケット化手段は、前記優先データから抽出したデータを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、パ
ケット化情報を用いてパケットヘッダを生成するパケットヘッダ生成手段と、前記パケットヘッダとペイロードとを組み合わせるパケットを生成するパケット生
成手段とを含み、前記カウンタ手段は前記バッファ手段からペイロード長に相当
15 するデータを読み出すための制御データを出力する。

前記第 2 のパケット化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、パケット化情報を用いてパケットヘッ
ダを生成するパケットヘッダ生成手段と、前記データにエラー訂正を付加するエラー訂正付加手段と、前記パケットヘッダと前記エラー訂正を付加し
20 たデータとを合成するパケット合成手段とを含み、前記カウンタ手段は前記バッファ手段よりペイロード長に相当するデータを読み出すための制御データを出力する。

前記優先データおよび前記一般データが処理されるレイヤよりも下位レイヤの受信フレームを処理するレイヤにおいて、前記受信フレームに含まれる受信パ
ケットの通信プロトコルヘッダから前記優先データと前記一般データを選別して、
25 前記優先データの処理と前記一般データの処理を独立に行う。

前記第 2 のパケット化手段は、暗号鍵切替手段を含み、前記暗号鍵切替手段に
入力される暗号鍵を指定されたタイミングで切り替えながら前記暗号化手段に入
力し、前記暗号化手段における暗号化鍵を指定の間隔で切替る。

5 前記暗号鍵切替に用いるタイミングとしては、前記パケットヘッダ生成手段の
出力であるパケットヘッダ内の所定のシーケンス番号に同期して発生したタイミ
ングである。

前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケッ
トが H T T P を使用している場合、H T T P リクエスト毎に更新される。

10 また、前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信
パケットが H T T P を使用している場合、一定のデータ量毎に変化される。

または、前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送
信パケットが R T P を使用している場合、予め決められた期間内に更新される。

前記暗号鍵切替に用いるタイミングとしては、エラー訂正マトリックスの終点
または始点に同期して発生したタイミングである。

15 本発明によれば、上記課題を解決するために、ネットワークを介して論理的に
接続されたパケット送受信装置は、M P E G - T S などの送信データの機密性お
よび著作権の保護を実現するための認証・鍵交換手段（A K E 手段）と、送信デ
ータを暗号化する暗号化手段と、送信データを用いて送信パケットを生成するパ
ケット化手段と、暗号化された送信データを復号する復号手段と、送信パケット
20 の送信先からフィードバックされるパケット受信状況に基づいて適切なパケット
送信条件を設定する送信条件設定管理手段と、パケット受信手段と、受信条件設
定管理手段とを備える。

これにより、D T C P 方式をインターネットの標準プロトコルである I P プロ
トコルに実装することができる。

25 また、M P E G - T S などの A V データを送信装置で暗号化してデータの機密
性および著作権の保護などを図り、パケット（例えば、I P パケット）を伝送可

能なネットワークを介して伝送し、受信装置で暗号化されたデータを復号することが可能である。

本発明のある実施の形態によれば、パケット化手段において、送信パケットを一般パケットと、リアルタイム性が高く、優先的に送信されるべき優先パケットとにクラス分けし、一般パケットを第1のデータキュー手段に、また、優先パケットを第2のデータキュー手段に入力する。そして、送信キュー制御手段は、第1のデータキュー手段および第2のデータキュー手段に一時的に蓄積されているパケットの送信順序を制御する。これにより、データの機密性および著作権の保護を図りながら、リアルタイム性の高いデータを優先的に伝送することができる。

また、入力ストリームが2チャンネル以上の複数ストリームである場合、各々のストリームに関係する信号を優先データと一般データにクラス分けしてもよい。

本発明のある実施の形態によれば、パケット化手段は、第1のパケット化手段と第2のパケット化手段とを含んでいる。第1のパケット化手段には、A K E 関連情報を含む一般データが入力される。第2のパケット化手段には、暗号化手段にて生成された暗号化送信データおよびA K E 関連情報が入力される。第2のパケット化手段では、ハードウェアによってパケットが生成される。なお、A K E 関連情報とは、コピー制御情報または暗号化鍵更新情報のことである。

第1のパケット化手段にて生成されたパケットは、第1のデータキュー手段に入力されて一時的に蓄積され、第2のパケット化手段にて生成されたパケットは第2のデータキュー手段に入力されて、一時的に蓄積される。

送信条件設定管理手段が、送信キュー制御手段に、第2のデータキュー手段に一時的に蓄積されているパケットを優先的に出力するように命令すると、暗号化されたデータが優先的に出力される。この制御において、第2のデータキュー手段がオーバフローしないように制御し、受信装置が適切な大きさのバッファを有する場合、送信装置と受信装置との間でコンテンツのリアルタイム伝送が実現できる。

以上、送信装置と受信装置との間でデータを暗号化してリアルタイム伝送する場合に、第2の packets 化手段はハードウェアで構成されているため、ソフトウェア処理が間に合わないために発生する送信 packets の送り残しおよび受信 packets の取りこぼしといった不具合が発生しない。また、データ量の小さい第1の packets 化手段は安価なマイコンなどでも構成できるため、低コスト化を図ることができる。

本発明のある実施の形態によれば、機器認証と暗号化鍵の交換を行なう AKE 手段は、D T C P 方式に基づいた方式であり、暗号化鍵生成手段と、D T C P 情報生成手段と、AKE コマンド送信処理手段と、AKE コマンド受信処理手段と、交換鍵生成手段と、暗号化鍵変更情報生成手段と、復号鍵生成手段とを備える。暗号化鍵生成手段は、暗号化鍵を生成し暗号化に入力し暗号化動作を設定する。D T C P 情報生成手段は、外部から入力されるコピー制御情報、および、暗号化鍵生成手段から入力される鍵更新情報とを用いて、AKE 関連情報を生成する。AKE コマンド送信処理手段は、暗号化鍵生成手段より暗号化鍵を、外部より A K E パラメータを、さらに A K E コマンド受信処理手段より A K E コマンド情報を受け取り、A K E 送信コマンドを生成し出力する。A K E コマンド受信処理手段は、第1の packets 受信手段より A K E 設定制御情報を受け取り、A K E 送信処理手段、交換鍵生成手段、暗号化鍵変更情報生成手段にそれぞれ設定制御情報を出力する。暗号化鍵変更情報生成手段は、A K E コマンド受信処理手段と第1の packets 受信手段より情報を得て暗号化鍵変更情報を生成する。復号鍵生成手段は、交換鍵生成手段と暗号化鍵変更情報生成手段からの情報を用いて、復号鍵を生成し復号手段に出力する。

本発明のある実施の形態によれば、暗号化手段にて生成された暗号化送信データ、および、コピー制御情報および暗号化鍵更新情報などの A K E 関連情報が入力される第2の packets 化手段が、内部にエラー訂正符号付加手段を備え、これらの情報にエラー訂正符号を付加し、U D P / I P プロトコルにより伝送される。

これにより、IPパケットの伝送において、ネットワークでパケットロスおよびビットエラーなどが発生した場合にも、受信装置でエラー訂正により送信データの復元が可能となる。

本発明のある実施の形態によれば、優先して送信される優先パケットと、この優先パケットよりも送信優先度が低い一般パケットとを時間軸上で多重して送信し、送信される優先パケットにおける優先データの平均送信データレートを、たとえば、専用ハードウェアを用いて平均入力レート以上の速度で送信するように制御する。

また、一般データは一時的にバッファ手段に蓄積され、優先データ伝送が優先して行なわれる中で間欠的に伝送される。ここで、一般データの伝送レートが1Mbps以下の場合は、安価なCPUまたはマイコンなどのプロセッサを用いて一般伝送の伝送処理が可能である。

なお、ストリームとして入力される優先データでは、ストリームの無効データ部が除去され、有効データのみを用いて、パケット化情報に基づいてパケットが生成される。ここで、通信プロトコルとしてUDP/IPを使用すると、ヘッダとしては、アドレスとしてIPアドレス、また、サブアドレスとしてUDPポート番号を使用することとなる。

本発明のある実施の形態によれば、有効データから優先データフォーマット情報を得て、外部から入力されるパケット化情報と共にパケット化パラメータの決定に使用する。これにより、たとえば、優先データがDV系の場合はDIFブロックの80バイト単位、また、MPEG系の場合はTSパケットの188バイト単位で優先データのパケット化の自動化などを行なうことができ、送受信装置の構成を簡単にすることができる。

本発明のある実施の形態によれば、送信装置内の優先データパケット化手段において、優先データにエラー訂正符号を付加することにより、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データを復元することが

できる。

本発明のある実施の形態は、送信装置内の優先データパケット化手段における伝送エラー保護機能に関し、優先データを暗号化した後、エラー訂正符号を付加することにより、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データを復元することが可能になるとともに、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ（ＡＶデータ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるＡＶデータの販売、課金が可能となり、安全性の高いＢ－Ｂ、Ｂ－Ｃのコンテンツ販売流通が可能となる。

本発明のある実施の形態は、暗号化を行なう暗号鍵を切り替える方法に関し、エラー訂正マトリックスの位相を暗号鍵の切替位相とすることにより、暗号鍵の切替をスムーズに実行することが可能となる。

本発明のある実施の形態は、有効データパケットのパケットヘッダのポート番号設定に関し、優先データのフォーマットまたはチャネル番号とポート番号の組み合わせを決めるテーブルを送信装置および受信装置で設けることにより、受信装置でポート番号を検出するだけでフォーマット検出ができるため、受信装置での信号処理を簡単にすることが可能となる。

また、２系統のストリーム処理が可能な受信装置で２つのストリームを同時受信している場合でもポート番号でフォーマットまたはチャネルの識別が可能となる。

図面の簡単な説明

図１は、本発明を適用可能なシステムの一例を示す図である。

図２は、認証および鍵交換にＤＴＣＰ方式を適用する場合の送信装置および受信装置の動作を示すための図である。

図 3 は、D T C P方式をイーサネット（R）を用いて、2階建ての家屋に適用した場合の一例を示す模式図である。

図 4 は、本発明の実施の形態 1 によるパケット送受信装置のブロック図である。

図 5 は、M P E G - T Sを用いて、パケットさらには、フレームを生成して、
5 伝送する場合のパケット形式の一例を示す模式図である。

図 6 は、本発明の実施の形態 1 によるプロトコルスタックを説明するための模式図である。

図 7 は、本発明の実施の形態 2 によるパケット送受信装置のブロック図である。

図 8 は、本発明の実施の形態 3 によるパケット送受信装置のブロック図である。

10 図 9 は、本発明の実施の形態 3 によるプロトコルスタックによる説明図である。

図 1 0 は、M P E G - T Sを用いて、パケットさらには、フレームを生成して、伝送する場合のパケット形式の一例を示す模式図である。

図 1 1 は、本発明の実施の形態 4 のパケット送受信装置のブロック図である。

図 1 2 は、本発明の実施の形態 4 におけるパケット化手段およびパケット受信
15 手段を説明するためのブロック図である。

図 1 3 は、本発明の実施の形態 5 におけるパケット化手段およびパケット受信手段を説明するためのブロック図である。

図 1 4 は、本発明の実施の形態 5 のプロトコルスタックの模式図である。

図 1 5 は、エラー訂正方式がリードソロモン方式である場合の模式図である。

20 図 1 6 は、エラー訂正方式がパリティ方式である場合の模式図である。

図 1 7 は、本発明の実施の形態 6 によるパケット送受信装置のブロック図である。

図 1 8 は、本発明の実施の形態 6 の別の形態によるパケット送受信装置のブロック図である。

25 図 1 9 は、本発明の実施の形態 7 によるパケット送信手段のブロック図である。

図 2 0 は、優先パケットのプロトコルスタックの模式図である。

図 2 1 は、優先パケットと一般パケットの伝送タイミングの模式図である。

図 2 2 は、本発明の実施の形態 7 の変形例によるパケット送信手段のブロック図である。

図 2 3 は、本発明の実施の形態 8 によるパケット送信手段のブロック図である。

5 図 2 4 は、本発明の実施の形態 8 の変形例によるパケット送信手段のブロック図である。

図 2 5 は、本発明の実施の形態 9 によるパケット送信手段のブロック図である。

図 2 6 は、本発明の実施の形態 9 の変形例による優先データパケット化手段のブロック図である。

10 図 2 7 は、本発明の実施の形態 9 の別の変形例による優先データパケット化手段のブロック図である。

図 2 8 は、エラー訂正がパリティ処理方式の場合のパケット構成を示す図である。

15 図 2 9 は、エラー訂正がリードソロモン方式の場合のパケット構成を示す図である。

図 3 0 は、本発明の実施の形態 1 0 のパケット送信手段のブロック図である。

図 3 1 は、本発明の実施の形態 1 0 の優先データパケット化手段のブロック図である。

20 図 3 2 は、本発明の実施の形態 1 1 の優先データパケット手段のブロック図である。

図 3 3 は、暗号の切り替えタイミングを説明するための模式図である。

図 3 4 は、本発明の実施の形態 1 2 による優先データパケット手段のブロック図である。

25 図 3 5 は、本発明の実施の形態 1 3 による I E E E 1 3 9 4 ストリーム伝送に適用したパケット送信システムのブロック図である。

図 3 6 は、本発明の実施の形態 1 3 による S D I / S D T I / D V B - A S I

ストリームの伝送に適用したパケット送信システムのブロック図である。

図 3 7 は、本発明の実施の形態 1 3 のパケット送受信装置のブロック図である。

図 3 8 は、D T C P 方式を用いて、M P E G - T S を、I E E E 1 3 9 4 規格に準拠する伝送メディアを介して伝送することを示す模式図である。

5

発明を実施するための最良の形態

本願明細書の以下の説明において、パケットを含む情報を送信および受信可能な装置を送受信装置とよぶ。2つの送受信装置はお互いに情報を通信する。また、本願明細書の以下の説明では、便宜上、送信すべきデータ（例えば、A V データ）を送信する送受信装置を「送信装置」とよび、送信装置によって送信されたそのようなデータを受信する送受信装置を「受信装置」とよぶ。

10

まず、始めに、本発明を明確にするために本発明を適用可能なシステムの概略について説明する。

図 1 は、本発明を適用可能なシステムの一例を示す図である。

15

送信装置 1 0 1 は、データをルータ 1 0 2 を介して、受信装置 1 0 3 に送信する。

より詳細には、送信装置 1 0 1 には、送受信条件関連情報、認証・鍵交換（A u t h e n t i f i c a t i o n a n d K e y E x c h a n g e、以下、A K E とよぶ）設定情報、入力ストリーム（M P E G - T S などのデータ）が入力され、以下の手順 1 から手順 3 に基づいて、通信が実行される。

20

手順 1）送受信パラメータの設定：

（1 - 1）送信装置 1 0 1 および受信装置 1 0 3 の M A C （M e d i a A c c e s s C o n t r o l）アドレス、I P （I n t e r n e t P r o t o c o l）アドレス、T C P / U D P （T r a n s m i s s i o n C o n t r o l P r o t o c o l / U s e r D a t a g r a m P r o t o c o l）ポート番号等を設定する。

25

(1-2) 送信信号の種別、帯域を設定する。

送信装置101および受信装置103は、QoS (Quality of Service) エージェントとして機能し、ルータ102は、QoSマネージャとして機能する。QoSエージェントとQoSマネージャとの間でIEEE 802.1Q (VLAN) 規格を用いたネットワークに関する設定が行われる。

(1-3) IEEE 802.1Q/p 規格に基づいて優先度が設定される。

手順2) 認証および鍵交換：

(2-1) 送信装置101および送信装置103は、お互いを認証し、お互いに鍵を交換する。この場合、例えば、DTCP方式を用いることもできる。

手順3) データ伝送：

(3-1) 送信装置101から受信装置103に暗号化されたデータ（例えば、MPEG-TS）が伝送される。

なお、図1では、入力ストリームとして、MPEG-TSが送信装置101に入力されているが、本発明は、これに限定されない。このような入力ストリームとしては、例えば、MPEG1/2/4などのMPEG-TSストリーム (ISO/IEC 13818)、DV (IEC 61834、IEC 61883)、SMPTE 314M (DV-based)、SMPTE 259M (SDI)、SMPTE 305M (SDTI)、SMPTE 292M (HD-SDI) 等で規格化されたストリームがある。

なお、送信装置101から送信されるデータとしては、一般的なAVデータであってもよい。さらに、本発明のデータは、ファイルであってもよい。データとしてファイルを転送する場合、送信装置101と受信装置103との間の伝播遅延時間と、送信装置101と受信装置103のそれぞれの処理能力との関係から、データ転送速度がAVデータの通常再生データレートよりも大きくなるなどの条件下において、リアルタイムよりも高速にデータを伝送することが可能になる。

次に、図2を参照して、上記手順2の認証および鍵交換に関して、さらに詳細

に説明する。

図 2 は、認証および鍵交換に D T C P 方式を適用する場合の送信装置および受信装置の動作を示すための図である。

ここでは、D T C P 方式に準拠した認証と鍵交換 (A u t h e n t i f i c a
5 t i o n a n d K e y E x c h a n g e、以下、A K Eともよぶ) が行な
われている。その場合、送信装置 1 0 1 を A K E ソースともよび、受信装置 1 0
3 を A K E シンクともよぶ。

送信装置 1 0 1 と受信装置 1 0 3 との間は I P ネットワークにより接続されて
いる。

10 まず、送信装置 1 0 1 から受信装置 1 0 3 にデータのコピー保護情報を含んだ
データの保護モード情報が送信される。ここで、送信装置 1 0 1 は、暗号化デー
タを同時に送信してもよい。

受信装置 1 0 3 は、データのコピー保護情報を解析し、使用する認証方式を決
定して認証要求を送信装置 1 0 1 に送る。これらの動作を行うことによって、送
15 信装置 1 0 1 および受信装置 1 0 3 は認証鍵を共有する。

次に、送信装置 1 0 1 は認証鍵を用いて交換鍵を暗号化することによって、暗
号化交換鍵を生成し、送信装置 1 0 1 は、暗号化交換鍵を受信装置 1 0 3 に送信
する。受信装置 1 0 3 は、送信装置 1 0 1 と共有している認証鍵を用いて、暗号
化交換鍵を復号して、交換鍵を生成する。

20 次いで、送信装置 1 0 1 は暗号化鍵を時間的に変化させるために、時間ととも
に変更する鍵変更情報を生成する。ここで、この鍵変更情報は、シード情報とも
よばれる。送信装置 1 0 1 は、鍵変更情報を受信装置 1 0 3 に送信する。

送信装置 1 0 1 は、交換鍵と鍵変更情報とを用いて暗号化鍵を生成して、デー
タ (例えば、M P E G - T S) をこの暗号化鍵を用いて暗号化手段で暗号化する
25 ことによって、暗号化データを生成し、この暗号化データを受信装置 1 0 3 に送
信する。

受信装置 103 は、鍵変更情報と交換鍵とを用いて、暗号化鍵を生成する。受信装置 103 ではこの暗号化鍵を用いて暗号化データを復号する。受信装置 103 において暗号化鍵を復号鍵ともよぶ。

なお、送信装置 101 および受信装置 103 は、その後、任意の時間にお互いの鍵変更情報を確認してもよい。

図 3 は、D T C P 方式をイーサネット (R) を用いて、2 階建ての家屋に適用する場合の一例を示す模式図である。

1 階のネットワーク構成 301 は、ルータ 303 を含んでおり、ルータ 303 は、1 階に設置されている。1 階のネットワーク構成 301、100Mbps の F T T H (F i b e r t o t h e H o m e) を介してインターネットに接続されている。

2 階のネットワーク構成 302 は、スイッチングハブ 304 を含んでおり、スイッチングハブ 304 は、2 階に設置されている。

ルータ 303 は、ネットワーク 305 を介して、スイッチングハブ 304 に接続されており、それにより、1 階のネットワーク構成 301 は、2 階のネットワーク構成 302 に接続されている。ここで、ネットワーク 305 は、ルータ 303 とスイッチングハブ 304 とを接続するイーサネット (R) ネットワークであり、ルータ 303 は、スイッチングハブとしても機能している。

家屋の全てのイーサネット (R) ネットワークのデータレートは 100Mbps である。

1 階のネットワーク構成 301 では、ルータ 303 には、テレビ (TV (T e l e v i s i o n))、パソコン (PC (P e r s o n a l C o m p u t e r)) および DVD (D i g i t a l V e r s a t i l e D i s c) レコーダが 100Mbps のイーサネット (R) で接続され、また、エアコンおよび冷蔵庫が E C H O N E T で接続されている。

また、2 階のネットワーク構成 302 では、スイッチングハブ 304 には、テ

レビ (TV)、パソコン (PC) および DVD レコーダが 100Mbps のイーサネット (R) で接続され、また、エアコンが ECHONET で接続されている。ECHONET は「エコーネットコンソーシアム」 (<http://www.echonet.gr.jp/>) で開発された伝送方式である。

5 図 3 において、パソコン (PC)、DVD レコーダ、ルータ 303 およびスイッチングハブ 304 は、IEEE 802.1Q 規格 (VLAN) に対応している。したがって、各ポートのデータレートが全て同じ (例えば 100Mbps) である。ルータ 303 およびスイッチングハブ 304 において、特定の出力ポートから出力されるデータレートの合計がそのポートの出力ポートの伝送レートの
10 規格値または実効値を越えないかぎり、入力ポートから入力されたデータは、ルータ 303 またはスイッチングハブ 304 内部で失われることなく、全て出力ポートから出力される。

スイッチングハブ 304 に、たとえば 8 個の入力ポートを介してデータが同時に入力されても、それぞれのデータの出力ポートが異なっていれば、それぞれの
15 データは、ルータ 303 またはスイッチングハブ 304 の内部に設けられたバッファにおいて競合することなく、スイッチングされて出力ポートから出力される。したがって、入力ポートから入力されたデータはパケット落ちすることなく全て出力ポートから出力される。

図 3 では、家屋内の全てのイーサネット (R) のデータレートが 100Mbps
20 s であり、1 階と 2 階との間のネットワーク 305 のデータレートも 100Mbps である。1 階の機器と 2 階の機器との間で複数のデータが流れる場合、各データに対するデータレートの制限がないと、このネットワーク 305 上を流れるデータレートの合計が 100Mbps を越える可能性があり、MPEG-TS の映像アプリケーションなどのリアルタイムな伝送が必要とされるデータストリー
25 ムが途切れる可能性がある。

この場合、リアルタイムな伝送が必要とされるデータストリームが途切れない

ようにするには、伝送データに対して優先制御を行うことが必要である。端末だけでなく、ルータ 303 およびスイッチングハブ 304 に、後述するストリーム伝送およびファイル転送の速度制限機構などを導入することによって、リアルタイムな伝送が必要とされるデータストリームを途切れないようにすることができる。

例えば、リアルタイムな伝送が必要とされる MPEG-TS データの伝送優先度をファイルデータの伝送優先度よりも高くすると、1 階の PC と 2 階の PC との間でファイル転送を行いながら、同時に、1 階の DVD レコーダ、PC または TV と、2 階の DVD レコーダ、PC または TV との間で MPEG-TS データを暗号化してリアルタイムで伝送することが可能となる。

ルータ 303 またはスイッチングハブ 304 における伝送速度制限機構は、データ流入制御により実現できる。より具体的には、ルータ 303 またはスイッチングハブ 304 の入力データキュー手段において優先度の高いデータと低いデータとを比較して、優先度の高いデータを優先的に出力することにより実現できる。この優先制御方式に用いるバッファ制御ルールとしては、ラウンドロビン方式、流体フェアスケジューリング方式、重み付けフェアスケジューリング方式、自己同期フェアスケジューリング方式、WF F Q 方式、仮想時計スケジューリング方式、クラス別スケジューリング方式などがある。これらのスケジューリング方式に関する詳細は、戸田巖著、「ネットワーク Q o S 技術」、平成 13 年 5 月 25 日（第 1 版）、オーム社刊の第 12 章などに記述されている。

（実施の形態 1）

図 4 は、本発明の実施の形態 1 によるパケット送受信装置 401 のブロック図である。

パケット送受信装置 401 は、D T C P 方式に準拠した認証および鍵交換を行い、パケットを送信および受信する。ここで、パケット送受信装置 401 は、パ

ケット送受信装置 401 と同様の機能を有する別のケット送受信装置にケットを送信し、そのようなケット送受信装置からのケットを受信することを想定している。したがって、ケット送受信装置 401 は、送信ケットの到着先に送信ケットを送信し、受信ケットの送信元から受信ケットを受信する。

5 ケット送受信装置 401 は、暗号化鍵および復号鍵を生成する認証・鍵交換手段（以下、AKE手段ともよぶ）402 と、暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段406 と、送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも1つを用いて、送信ケットの送信条件を設定するための送信条件設定情報を生成する送信
10 条件設定管理手段404 と、暗号化送信データを用いて、送信ケットを生成するケット化手段403 と、受信条件関連情報およびケット受信情報の少なくとも一方を用いて、受信ケットの受信条件を設定するための受信条件設定情報を生成する受信条件設定管理手段408 と、受信ケットを受信するケット受
15 信手段405 であって、受信条件設定情報を用いて、受信ケットから、受信ケットに含まれる受信データを抽出するとともに、受信ケットからケット受信情報を生成し、ケット受信情報を認証・鍵交換手段402 または受信条件設定管理手段408 に出力する、ケット受信手段405 と、復号鍵を用いて受信データを復号する復号手段407 とを備える。

20 ケット送受信装置 401 は、送信ケットを用いて送信フレームを生成するフレーム化手段409 と、受信フレームを受信するフレーム受信手段410 とをさらに備えており、それにより、ケット送受信装置 401 は、送信ケットを含む送信フレームを送信する送信装置として機能するとともに、受信ケットを含む受信フレームを受信する受信装置としても機能する。

25 以下に、ケット送受信装置 401 が、TCP/IP または UDP/IP などを用いて送信フレームを送信する場合について説明する。

送信条件設定管理手段 404 には、送信条件関連情報と、送受信管理情報と、

受信条件設定情報とが入力される。

送信条件関連情報は、例えば、送信データの種別と、送信先アドレスまたはポート番号の情報と、送信に用いるパス情報（ルーティング情報）と、送信データの帯域と、送信データの送信優先度とを含む。

- 5 送受信管理情報は、送信装置（ローカル）および受信装置（リモート）における機器管理制御データを含む。

- より詳細には、送信管理情報は、送信装置（ローカル）および受信装置（リモート）におけるMAC（Media Access Control）アドレスまたは位置情報などの機器管理制御データを含む。位置情報は、例えば、地域コード、住所、郵便番号、あるいは、経度・緯度などに範囲が指定された情報である。位置情報を用いて、認証を行う送信機器と受信機器との範囲を限定することが可能となる。また、送信装置と受信装置との間で送受信されるパケットの片道または往復の伝播時間があらかじめ決められた制限時間より短い時間である場合に、認証を許可することにより認証範囲を制限することも可能である。たとえば、
10 Ethernet方式のIP接続で、RTT（Round Trip Time）が1msec以下である場合にのみ認証を許可することにより認証の範囲を制限することができる。また、802.11a規格または802.11b規格などの無線方式とEthernet規格などの複数の伝送メディアを組み合わせた場合には、それぞれの伝送メディアの伝播遅延特性に応じたRTTを設定して認
15 証を許可することができる。これらの時間の測定は、たとえば、AKEの専用コマンドで行ってもよいし、図5を参照して以下に説明するように、パケット付加情報がタイムスタンプまたは位置情報を含むことによって実現することもできる。
20

- さらに、送信装置と受信装置との間の送受信区間において無線伝送区間が存在する場合、その無線伝送区間ではデータを無線LANのセキュリティ方式である
25 WEPまたはWPA方式によって、データの暗号化およびスクランブル化を行い伝送するモードであることを確認した後に、認証を許可することにより、無線伝

送区間でのデータ漏洩による第3者によるデータ解読を防止することができる。

受信条件設定情報は、受信装置の受信状況を受信装置から送信装置にフィードバックする情報を含む。この情報は、受信条件設定管理手段408から送信条件設定管理手段404に入力される。

5 送信条件設定管理手段404は、送信条件関連情報と、送受信管理情報と、受信条件関連情報との少なくとも1つを用いて、送信条件設定情報を生成する。送信条件関連情報は、パケット送受信装置の位置情報と、送信パケットの到着先の位置情報または受信パケットの送信元の位置情報との少なくとも一方を含んでいる。

10 送信条件設定管理手段404にて生成された送信条件設定情報を用いて、パケット化手段403およびフレーム化手段409では、ヘッダおよびペイロードなどが設定される。送信条件設定管理手段404は、また、送信条件設定情報をパケット化手段403、および、パケット化手段403に含まれるパケット付加情報生成手段411に出力する。

15 AKE手段402には、認証・鍵交換設定情報（以下、AKE設定情報ともよぶ）が入力される。AKE手段402から、このAKE設定情報に関連した認証・鍵交換関連情報（以下、AKE関連情報ともよぶ）がパケット付加情報生成手段411に入力される。認証・鍵交換関連情報は、例えば、伝送時における暗号化送信データの暗号化状態を表すコピー保護情報と、暗号化鍵変更情報とを含む。

20 暗号化手段406には、例えば、MPEG-TSが、入力ストリームとして入力される。暗号化手段406は、MPEG-TSの一部を送信データとし、AKE手段402にて生成された暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する。暗号化送信データは、暗号化手段406から
25 パケット化手段403に出力される。

パケット化手段403は送信条件設定管理手段404において生成された送信

条件設定情報に基づいて、暗号化送信データを用いて、送信パケットを生成する。

パケット化手段403は、パケット付加情報生成手段411を含み、パケット付加情報生成手段411は、送信条件設定情報および認証・鍵交換関連情報の少なくとも1つを用いてパケット付加情報を生成する。

5 パケット化手段403は、暗号化送信データを所定の大きさに変換し、IETFでIPv4またはIPv6として規定されているIP（Internet Protocol）ヘッダを付加してもよく、IPv4ヘッダのサービスタイプフィールド、または、サービスタイプフィールド内のTOS（Type of Service）フィールドに優先パケットであることを示す情報を付加してもよく、また、IPv6ヘッダのプライオリティフィールドに優先パケットであることを示す情報を付加してもよい。

10 パケット付加情報生成手段411にて生成されたパケット付加情報は、パケット化手段403に入力され、暗号化送信データに付加される。より具体的には、パケット付加情報は、TCP/IPまたはUDP/IPプロトコルのヘッダの一部として暗号化送信データに付加され、送信パケットが生成される。

15 送信パケットには、また、AKE手段402におけるDTCP方式のコピー制御情報として、暗号化モード情報が付加される。

20 送信パケットは、さらに、フレーム化手段409においてMACヘッダが付加されて、イーサネット（R）フレームが生成され、イーサネット（R）フレームは、送信フレームとしてフレーム化手段409からネットワークに出力される。

 なお、コンテンツのコピー制御情報をCGI（Copy Control Information）、伝送における暗号化を表すコピー保護情報をEMI（Encryption Mode Indicator）とよぶ。一般的には、EMIはCGIと同等またはより強い保護モードが用いられる。

25 次に、パケット送受信装置401が受信フレームを受信する場合について説明する。

フレーム受信手段410は、ネットワークを介して受信フレームを受信する。
フレーム受信手段410は、受信フレームに含まれるMACヘッダを抽出し、抽出したMACヘッダに基づいてフィルタリングを行い、フィルタリングによって得られたIPパケットをパケット受信手段405に出力する。

- 5 パケット受信手段405では、IPパケットのIPパケットヘッダなどを識別することによって、フィルタリングを行い、パケット受信情報を生成する。フィルタリングによって、パケット受信情報として得られたAKE情報は、パケット受信手段405に含まれるパケット付加情報抽出手段412に入力される。パケット付加情報抽出手段412は、受信パケットからパケット付加情報を抽出し、
10 抽出したパケット付加情報はAKE手段402に出力される。

このように、送信装置のAKE手段と、受信装置のAKE手段とは、ネットワークを介して1対1に接続することができるので、通信プロトコルを介してお互いにメッセージを交換することができる。

- 15 AKE手段402は、パケット送受信装置401の位置情報と、送信パケットの到着先の位置情報または受信パケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可する。

- 20 AKE手段402は、例えば、パケット送受信装置401と、送信パケットの到着先または受信パケットの送信元との間で、パケット送受信装置401から送信パケットの到着先または受信パケットの受信元までの片道または往復の伝播時間があらかじめ決められた制限時間より短い時間である場合に、認証を許可する。

あるいは、AKE手段402は、パケット送受信装置401と、送信パケットの到着先または受信パケットの送信元との間の送受信区間において無線伝送区間が存在する場合、無線伝送区間ではデータをスクランブルして伝送するモードであることを確認する場合に、認証を許可してもよい。

- 25 したがって、二つのAKE手段の設定手順に従い、認証および鍵交換を実行することができる。

送信装置として機能するパケット送受信装置と、受信装置として機能するパケット送受信装置との間で認証および鍵交換が成立した後、送信装置は、暗号化したAVデータを送信する。

送信装置としては、MPEG-TSデータが暗号化手段406に入力され、暗号化手段406は、MPEG-TSを暗号化した暗号化MPEG-TSデータを生成する。この暗号化MPEG-TSデータは、パケット化手段403に入力され、パケット化手段403においてTCP/IPプロトコルのヘッダが付加されて、送信パケットが生成される。

フレーム化手段409では、802.1Q (VLAN) 方式を用いて、送信パケットにさらにMACヘッダが付加されて、イーサネット (R) フレームに変換され、送信フレームが生成される。このように生成された送信フレームは、ネットワークに出力される。

ここで、MACヘッダ内のTCI (Tag Control Information) 内のPriority (ユーザ優先度) を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。

受信装置では、ネットワークより入力する信号がフレーム受信手段410でMACヘッダを元にフィルタリングされ、IPパケットとしてパケット受信手段405に入力される。パケット受信手段405でパケットヘッダなどの識別によりフィルタリングされ、復号手段407に入力され、復号されたMPEG-TSが出力される。

なお、送信条件設定管理手段404には、受信条件設定管理手段408から受信条件設定情報として、受信状況を送信装置にフィードバックするための情報が入力され、送信条件設定管理手段404は、これに基づいて、送信条件設定情報を生成し、送信条件設定情報に基づいて、パケット化手段403およびフレーム化手段409で生成するヘッダおよびペイロードが設定される。

図5は、MPEG-TSを用いてパケット、さらには、フレームを生成して、

伝送する場合の packets 形式の一例を示す模式図である。ここで、MPEG-TS は、ISO/IBC 13818 に準拠している。また、MPEG-TS は、ARIB 規格、ARIB TR-B14、ARIB TR-B15、または、ARIB STD-B21 に基づく信号形式でもよい。

5 入力ストリームとして入力される MPEG-TS は、188 バイト毎に分断され、188 バイトの MPEG-TS には 6 バイトのタイムコード (TC (Time Code)) が付加されて、194 バイトの単位が形成される。ここで、TC は、42 ビットのタイムスタンプと 6 ビットのベースクロック ID (BCID (Base Clock ID)) とを含んでいる。

10 BCID によって、タイムスタンプの周波数情報を表すことができる。

例えば、

(ケース 1) BCID が 0x00 の場合は、タイムスタンプの周波数情報はない、

(ケース 2) BCID が 0x01 の場合は、タイムスタンプの周波数情報としては 27 MHz (MPEG2 のシステムクロック周波数) である、

15 (ケース 3) また、BCID が 0x02 の場合は、タイムスタンプの周波数情報としては 90 kHz (MPEG1 で使用されるクロック周波数) である、

(ケース 4) BCID が 0x03 の場合は、タイムスタンプの周波数情報としては 24.576 MHz (IEEE 1394 で使用されるクロック周波数) である、

20 (ケース 5) BCID が 0x04 の場合は、タイムスタンプの周波数情報としては 100 MHz (イーサネット (R) で使用される周波数) である。

194 バイト単位のデータを 2 つあわせて暗号化して暗号化データが生成され、さらに、その暗号化データに 7 バイトの packets 付加情報を付加すると、RTP プロトコルのペイロードが形成される。

25 ここでは、packets 付加情報は、2 ビットの EMI (Encryption Mode Indicator) と、1 ビットの O/E (Odd/Even) と

13ビットのReserved Dataと、40ビットのタイムスタンプまたは位置情報を含んでいる。EMIおよびO/EはDTCP方式で規定されている。なお、O/Eの代わりに、DTCPのシード情報(Nc)を用いてもよい。

5 パケット付加情報生成手段411(図4参照)が、AKE関連情報を用いて、EMIおよびO/Eを生成する。

タイムスタンプまたは位置情報は、送信条件設定情報を用いてパケット付加情報生成手段411(図4参照)にて生成された情報であり、Reserved Dataの後に続けて配置されている。タイムスタンプまたは位置情報は、また、O/EとReserved Dataとの間に配置されてもよい。

10 位置情報は、例えば、地域コード、住所、郵便番号、または、経度・緯度により範囲が指定された情報である。

ここでは、パケット付加情報は7バイトであったが、パケット付加情報は7バイトに限定されるものではない。

15 パケット付加情報は、タイムスタンプまたは位置情報を含んでなくてもよい。その場合、パケット付加情報は、2バイトとなる。

暗号化データに7バイトのパケット付加情報を付加すると、RTPプロトコルのペイロードが形成され、ヘッダとしてRTPヘッダが付加されると、RTPプロトコルが形成される。

20 RTPプロトコルは、TCPパケットまたはUDPパケットのペイロードであり、ヘッダとして、TCPヘッダまたはUDPヘッダが付加されると、TCPパケットまたはUDPパケットが形成される。

TCPパケットまたはUDPパケットは、IPパケットのペイロードであり、ヘッダとしてIPヘッダが付加されると、IPパケットが生成される。ここで、IPヘッダは、IETFでIPv4またはIPv6として規定されている。

25 さらにこのIPパケットはMACフレームのペイロードであり、ヘッダとしてイーサネットヘッダが付加されると、イーサネットパケットが生成される。

イーサネット（R）ヘッダとしては、図5に示すように、標準的なイーサネット（R）ヘッダとIEEE 802.1Q（VLAN）により拡張されたイーサネット（R）ヘッダの両方が適用可能である。

5 標準的なイーサネットヘッダは14バイトであり、6バイトのDA（Destination Address）と、6バイトのSA（Source Address）と、2バイトの長さ／タイプを示す情報とを含む。

802.1Qで拡張されたイーサネットヘッダは18バイトあり、802.1Qで拡張されたイーサネットヘッダは、SAと長さ／タイプを示す情報との間に4バイトの802.1q拡張部が設けられている点で標準的なイーサネットヘッダと異なる。

802.1q拡張部は、2バイトのTPID（Tag Control ID）と、VLAN優先度を示す2バイトのTCI（Tag Control Information）とを含む。

15 TCIは、3ビットのPriority（User Priority）と、1ビットのCFI（Canonical Format Indicator）と、12ビットのVID（VLAN Identifier）とを含む。

Priorityの使用法は、ISO／IEC 15802-3で規定されており、このPriorityのフラグを用いて、イーサネット（R）フレームの優先度を設定することができる。

20 次に、図6のプロトコルスタックを参照して上記手順を更に詳細に説明する。

図6は、本発明の実施の形態1によるプロトコルスタックを説明するための模式図である。

図6の左端には、OSI（Open Systems Interconnection）モデルの階層を示している。この階層は、下層から順に、リンク層、ネットワーク層、トランスミッション層、アプリケーション層となっている。

まず、送信装置から受信装置に暗号化データがデータポートを介して、また、

データのAKE関連情報がAKEポートを介して送信される。

受信装置では、データのコピー保護情報を解析して、認証方式を決定し、認証要求を送信装置に送る。

次に、送信装置では、乱数が発生され、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力すると、認証鍵が生成される。

受信装置でも所定の処理を行うことによって認証鍵が生成され、それにより、送信装置および受信装置は認証鍵を共有する。

なお、ここで暗号化を行うために使用する情報は、例えば、送信装置の独自情報（機器ID、機器の認証情報、マックアドレスなど）、秘密鍵、公開鍵、外部から与えられた情報などを1つ以上組み合わせて生成した情報であり、DES方式またはAES方式などの暗号化強度の強い暗号化方式を用いることによって、強固な暗号化が可能である。

次いで、送信装置は認証鍵を用いて交換鍵を暗号化して暗号化交換鍵を生成し、暗号化交換鍵を受信装置に送信する。受信装置は、認証鍵を用いて、暗号化交換鍵を交換鍵に復号する。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵（復号鍵）を生成する。

なお、送信装置は、暗号化鍵を時間的に変化させるために、時間とともに変更する鍵更新情報を生成し、この鍵更新情報を受信装置に送信する。

送信装置では、コンテンツデータであるMPEG-TSは暗号化鍵により暗号化され、暗号化データが生成される。そして暗号化データは、前述したEMI、O/EとともにAVデータとしてTCP（またはUDP）パケットのペイロードとなり、TCP（またはUDP）パケットが生成される。さらにこのTCP（またはUDP）パケットはIPパケットのペイロードとして使用され、IPパケットが生成される。さらにこのIPパケットはMACフレームのペイロードとして使用され、イーサネット（R）MACフレームが生成される。

なお、MACは、イーサネット（R）の規格であるIEEE 802.3規格

だけでなく、無線LANの規格であるIEEE 802.11規格のMACにも適用できる。

イーサネット(R) MACフレームは、イーサネット(R)上を送信装置から受信装置に伝送される。受信装置は、所定の手順に従って暗号化鍵(復号鍵)を生成する。そして、受信したイーサネット(R) MACフレームからIPパケットをフィルタリングする。さらにIPパケットからTCP(またはUDP)パケットを抽出する。そして、TCP(またはUDP)パケットからAVデータを抽出し、交換鍵と鍵変更情報を用いて生成された暗号化鍵(復号鍵)により、データ(MPEG-TS)が復号される。

AKE手段402が復号鍵を更新するタイミングを示すタイミング情報は、送信パケットに付加されていることが好ましい。その場合、AKE手段402が復号鍵を更新するタイミングは、送信パケットのTCPポート番号、またはUDPポート番号を変化させることによって通知されてもよい。

送信パケットがHTTPを使用している場合、AKE手段402が復号鍵を更新するタイミングは、HTTPリクエスト毎に更新されるか、または、一定のデータ量毎に変化されてもよい。

あるいは、送信パケットがRTPを使用している場合、AKE手段402が復号鍵を更新するタイミングは、予め決められた期間(例えば、60秒)内に更新されてもよい。

以上のように、MPEG-TSなどのデータを送信装置で暗号化して、HTTP/TCP/IPまたはRTP/UDP/IPなどにより、IPパケットをネットワークを介して伝送し、受信装置で元のデータに復号することが可能である。なお、前述したO/Eまたはシード情報(Nc)は、一定の規則、例えば、HTTPリクエスト毎、または、一定量のAVデータ毎(例えば、1MB毎)、あるいは、予め決められた一定時間内に更新すると、よりセキュリティを向上させることができる。

ここで、再び図3を参照して、スイッチングハブを用いたネットワークポートロジを変更することにより、ストリーム伝送とファイル転送を共存させることができることを説明する。

例えば、1階と2階との間のネットワーク305のデータレートを100Mbpsから1Gbpsに拡張することによって、1階のPCと2階のPCとの間でのファイル転送を行いながら、同時に、1階のDVDレコーダ、PCまたはTVと、2階のDVDレコーダ、PCまたはTVとの間でMPEG-TSを暗号化してリアルタイムで伝送することができる。

例えば、8つの100Mbpsのポートと、1つの1Gbpsのポートとを有する、市販されているスイッチングハブを用い、1階のネットワーク構成301と、2階のネットワーク構成302とを接続するネットワーク305に1Gbpsのポートを接続し、残りの8つの100MbpsのポートにTVなどのAV機器を接続する。100Mbpsのポートは8つなので、8つのポートにデータがそれぞれ最大100Mbpsで入力されて1つのポートから出力される場合であっても、入力ポートの合計データレートは $100\text{Mbps} \times 8\text{ch} = 800\text{Mbps}$ であり、1Gbpsより小さいため、8つの入力ポートから入力されたデータはスイッチングハブ内部で失われることなく、全て1Gbpsの出力ポートから出力される。

したがって、1階のAV機器から出力されるデータの全てを、ネットワーク305を介して、2階に伝送することが可能である。また、反対に、2階のAV機器から出力されるデータの全てを、ネットワーク305を介して1階に伝送することが可能である。

以上のようなスイッチングハブを用いることによって、データのリアルタイム伝送とファイル転送とを同時に行うことができる。

(実施の形態2)

図7は、本発明の実施の形態2によるパケット送受信装置401Aのブロック図である。

パケット送受信装置401Aは、送信キュー制御手段601と、第1のキュー手段602と、第2のキュー手段603とをさらに備える点を除いて、実施の形態1において図4を参照して説明したパケット送受信装置401と同様の構成を有している。以下の説明では、説明を簡略化する目的で、主に、送信キュー制御手段601と、第1のキュー手段602と、第2のキュー手段603について説明する。

パケット化手段403は、一般データにTCP/IPプロトコル処理をして、第1のパケットを生成し、第1のパケットを第1のキュー手段602に出力する。ここで、一般データとは、例えば、送信条件設定情報およびAKE関連情報である。

第1のキュー手段602は、第1のパケットを一時的に蓄積する。

パケット化手段403は、また、暗号化手段406にて生成された暗号化送信データにTCP/IPプロトコル処理をして、第2のパケットを生成し、第2のパケットを第2のキュー手段603に出力する。

第2のキュー手段603は、第2のパケットを一時的に蓄積する。

ここで、パケット化手段403は、一般データを用いて第1のパケットを生成しているのに対し、コンテンツデータである暗号化送信データを用いて第2のパケットを生成している。

送信キュー制御手段601は、送信条件設定情報に基づいて、第1のキュー手段602と第2のキュー手段603とにパケットが一時的に蓄積されている場合に、どちらのパケットを優先的に出力するかを制御する。

具体的には、送信キュー制御手段601は、第1のパケットまたは第2のパケットの送信経路に関する情報と、第1のパケットまたは第2のパケットを送信するのに必要な帯域幅に関する情報と、送信パケットの送信から到着までの遅延に

関する情報と、第1のケットまたは第2のケットの優先度に関する情報とのうち少なくとも1つの情報を用いて、第1のキュー手段に蓄積された第1のケットおよび第2のキュー手段に蓄積された第2のケットのいずれを送信するかを制御する。

5 送信キュー制御手段602は、通常状態では、一般データよりもMPEG-TSなどのコンテンツデータを優先的に出力するように第1のキュー手段602および第2のキュー手段603を制御する。すなわち、送信キュー制御手段602は、コンテンツデータである暗号化送信データを、一般データよりも優先させる優先データとして取り扱う。

10 優先データは、例えば、MPT 259M規格で規定された非圧縮SD方式信号、または、SMP 292M規格で規定された非圧縮HD形式、または、IEC 61883規格で規定されたIEEE 1394によるDVまたはMPEG-TSの伝送ストリーム形式、または、DVB規格A010で規定されたDVB-ASIによるMPEG-TS形式、MPEG-PS形式、MPEG-ES形式、MPEG-PES形式の内の少なくとも一つのデータストリーム形式である。

15 送信キュー制御手段601は、IETF rfc 2205、rfc 2208、rfc 2209で記載されたRSVP方式、IETF rfc 2210、rfc 2211、2212、rfc 2215で記載されたIntserv方式、IETF rfc 2474、rfc 2475、rfc 2597、rfc 2598で記載されたDiffServ方式のいずれか1つの制御方式を使用してもよい。

20 フレーム化手段409は、第1のキュー手段602または第2のキュー手段603からそれぞれ出力された第1のケットまたは第2のケットを用いて、送信フレームを生成し、ネットワークに送信フレームを出力する。

25 送信キュー制御手段601は、第1のキュー手段602から送信される第1のケットと第2のキュー手段603から送信される第2のケットとの間隔を平均化するように第1のキュー手段および第2のキュー手段を制御してもよい。

一般的に、送信装置から受信装置にMPEG-TSを低遅延で伝送する場合には、MPEG-TSのためのバッファも小さいため、オーバーフローが発生しやすい。

送信装置において、MPEG-TSのためのバッファ（例えば、第2のキュー手段603のバッファ）がオーバーフローしそうになった場合、あるいは、受信装置からフィードバックされた情報を参照して受信装置のMPEG-TSのためのバッファがアンダーフローしそうになったことが判明した場合には、MPEG-TSのデータを優先的に出力するように第2のキュー手段603の優先度を更に適応的に上げることにより、このようなバッファの破綻を回避することができる。

送信装置が受信装置を遠隔操作する場合において、受信装置の再生、停止などの制御応答をより速くするためには、送信装置において第1のキュー手段602の優先度を適応的に上げればよい。しかしながら、この場合には、MPEG-TSのためのバッファがオーバーフローまたはアンダーフローする可能性がある。

したがって、バッファのオーバーフローおよびアンダーフローを避け、かつ、受信装置の再生、停止などの制御応答をより速くするように送信装置が受信装置を遠隔操作するための態様としては、受信装置を遠隔制御するためのパケットをキュー手段を経由することなく、パケット化手段403から直接フレーム化手段409に出力することにより、迅速な制御応答を実現することができる。あるいは、受信装置を遠隔制御するためのパケットに対して第3のキュー手段を新たに設けることにより、迅速な制御応答を実現することができる。

受信装置の動作は実施の形態1と同様である。

送信キュー制御手段601は、第2のパケットのデータレートが所定の値より小さくならないように、第1のキュー手段602および第2のキュー手段603を制御することが好ましい。また、送信キュー制御手段601は、第2のキュー手段603に蓄積される時間があらかじめ決めた値より常に小さくなるように、

送信キュー制御手段 601 は第 1 のキュー手段 602 および第 2 のキュー手段 603 を制御することが好ましい。

(実施の形態 3)

5 実施の形態 3 について説明する。

図 8 は、本発明の実施の形態 3 によるパケット送受信装置 401B のブロック図である。

10 パケット化手段 403 が、第 1 のパケット化手段 701 と、第 2 のパケット化手段 702 とを含み、パケット受信手段 405 が、第 1 のパケット受信手段 703 と、第 2 のパケット受信手段 704 とを含む点を除いて、パケット送受信装置 401B は、実施の形態 2 において図 7 を参照して説明したパケット送受信装置 401A と同様の構成を有している。以下の説明では、説明を簡略化する目的で、主に、第 1 のパケット化手段 701 と、第 2 のパケット化手段 702 と、第 1 のパケット受信手段 703 と、第 2 のパケット受信手段 704 とについて説明する。

15 はじめに、この送受信装置 401B が送信フレームを送信する場合について説明する。

第 1 のパケット化手段 701 は、例えば、プロセッサを含んでおり、第 1 のパケット化手段 701 には、送信条件設定管理手段 404 にて生成された送信条件設定情報および AKE 関連情報が入力される。第 1 のパケット化手段 701 は、
20 プロセッサを用いたソフトウェア処理で送信条件設定情報および AKE 関連情報を TCP/IP プロトコル処理することによって、第 1 のパケットを生成する。第 1 のパケット化手段 701 は、第 1 のパケットを第 1 のキュー手段 602 に出力する。

25 第 1 のパケット化手段 701 は、IETF 文書で規定されているデータ処理プロトコルである RTCP, RTSP, HTTP, TCP, UDP, IP のうちの少なくとも 1 つのヘッダを付加する。

第2の packets 化手段702には、MPEG-TSなどの送信データを暗号化手段406にて暗号化した暗号化送信データが入力される。第2の packets 化手段702にはAKE関連情報が入力されてもよい。AKE関連情報は、例えば、コピー制御情報、暗号化鍵更新情報である。

5 第2の packets 化手段702はハードウェア処理によって、この暗号化送信データをUDP/IPプロトコル処理することによって、第2の packets を生成する。第2の packets 化手段702は、第2の packets を第2のキュー手段603に出力する。

10 第2の packets 化手段702は、データにシーケンス番号を付加するか、または、IETF文書で規定されているデータ処理プロトコルであるRTP、UDP、HTTP、TCP、IPのうちの少なくとも1つのヘッダを付加する。

15 送信キュー制御手段601は、第1のキュー手段602と第2のキュー手段603との両方に packets が一時的に蓄積されている場合、上述した実施の形態2と同様に、第1のキュー手段602および第2のキュー手段603のうちのどちらの packets を優先的に出力するかを制御する。

この送受信装置401Bが受信フレームを受信する場合について説明する。

フレーム受信手段410は、ネットワークを介して、受信フレームを受信する。フレーム受信手段410は、フレーム受信手段410を、MACヘッダに基づいて受信フレームからIP packets をフィルタリングする。

20 ここで、IP packets が、第1の packets 化手段701にて生成される第1の packets と同様の packets である場合、そのIP packets は第1の packets 受信手段703に入力され、IP packets が、第2の packets 化手段702にて生成される第2の packets と同様の packets である場合、そのIP packets は第2の packets 受信手段704に入力される。

25 第1の packets 受信手段703ではプロセッサを用いたソフトウェア処理でTCP/IPプロトコルの受信処理を行い、この処理によって生成された packets

ト受信情報をAKE手段402または受信条件設定管理手段408に出力する。

また、第2の packets 受信手段704ではハードウェア処理によりUDP/IPプロトコルの受信処理を行い、この処理によって抽出された受信データを復号手段407に出力する。復号手段407では、受信データの暗号が復号される。

5 次に、図9のプロトコルスタックを用い、上記手順を更に詳細に説明する。

図9は、本発明の実施の形態3によるプロトコルスタックを説明するための模式図である。

図9に示すプロトコルスタックは、MPEG-TSなどのAVデータのトランスミッション層がUDPである点を除いて、図6を参照して説明したプロトコルスタックと同様の構成である。したがって、以下の説明では、主にトランスミ
10 ション層がUDPである点について説明する。

送信装置において、コンテンツである送信データ（例えば、MPEG-TS）を暗号化鍵Kcを用いて暗号化することによって、暗号化送信データが生成される。暗号化送信データは、前述したEMI、O/EとともにAVデータとして、
15 ハードウェアによりUDPパケットのペイロードとなり、UDPヘッダを付加することによってUDPパケットが生成される。さらにこのUDPパケットはIPパケットのペイロードとして使用され、IPヘッダを付加することによって、IPパケットが生成される。

なお、送信装置から受信装置への、EMIおよびO/Eを伝送する方法としては、例えば、専用の別パケットを生成して伝送することも可能である。その場合、暗号化鍵の復号がさらに困難となり、コンテンツの盗聴、漏洩をより困難にできる。インターネットなどの公衆網においても、リアルタイムに伝送されるAVデータの暗号化パラメータを変化させたり、別パケットとして送ることによって、
20 コンテンツの盗聴、漏洩をより困難にすることができる。

25 管理制御データに関しては図6の例と同様に、ソフトウェア処理によりTCPパケットが生成され、IPパケットが生成される。

イーサネット（R）MACフレームは、イーサネット（R）上を送信装置から受信装置に伝送される。受信装置では、所定の手順に従って暗号化鍵を生成する。そして、受信したイーサネット（R）MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからUDPパケットが抽出され、UDPパケットから受信データが抽出され、暗号化鍵 K_c を用いて、受信データ（例えば、MPEG-TS）が復号される。

このように、暗号化送信データおよび一般データが処理されるレイヤよりも下位レイヤの受信フレームを処理するレイヤにおいて、受信フレームに含まれる受信パケットの通信プロトコルヘッダから優先データと一般データを選別して、優先データの処理と一般データの処理を独立に行うことができる。

図10は、MPEG-TSを用いてパケット、さらには、フレームを生成して、伝送する場合のパケット形式の一例を示す模式図である。ここでも、MPEG-TSは、ISO/IBC 13818に準拠している。

入力ストリームとして入力されるMPEG-TSは、188バイト毎に分断され、188バイトのMPEG-TSには6バイトのタイムコード（TC（Time Code））を付加されて、194バイトの単位が形成される。ここで、TCは、42ビットのタイムスタンプと6ビットのベースクロックID（BCID（Base Clock ID））とを含んでいる。

BCIDによって、タイムスタンプの周波数情報を表すことができる。

例えば、

（ケース1）BCIDが0x00の場合は、タイムスタンプの周波数情報はない、

（ケース2）BCIDが0x01の場合は、タイムスタンプの周波数情報としては27MHz（MPEG2のシステムクロック周波数）である、

（ケース3）また、BCIDが0x02の場合は、タイムスタンプの周波数情報としては90kHz（MPEG1で使用するクロック周波数）である、

（ケース4）BCIDが0x03の場合は、タイムスタンプの周波数情報として

は 24.576 MHz (IEEE 1394 で使用されるクロック周波数) である、

(ケース 5) BCID が 0x04 の場合は、タイムスタンプの周波数情報としては 100 MHz (イーサネット (R) で使用される周波数) である。

5 194 バイト単位のデータを 2 つあわせて暗号化して暗号化データが生成され、さらに、その暗号化データに 2 バイトの packets 付加情報を付加すると、RTP プロトコルのペイロードが形成される。

10 ここでは、packets 付加情報は、2 ビットの EMI (Encryption Mode Indicator) と、1 ビットの O/E (Odd/Even) と 13 ビットの Reserved Data と、40 ビットのタイムスタンプまたは位置情報を含んでいる。EMI および O/E は DTCP 方式で規定されている。なお、O/E の代わりに、DTCP のシード情報 (Nc) を用いてもよい。

 packets 付加情報生成手段 411 (図 4 参照) が、AKE 関連情報を用いて、EMI および O/E を生成する。

15 タイムスタンプまたは位置情報は、送信条件設定情報を用いて packets 付加情報生成手段 411 (図 4 参照) にて生成された情報であり、Reserved Data の後に続けて配置されている。タイムスタンプまたは位置情報は、また、O/E と Reserved Data との間に配置されてもよい。

20 位置情報は、例えば、地域コード、住所、郵便番号、または、経度・緯度により範囲が指定された情報である。

 ここでは、packets 付加情報は 7 バイトであったが、packets 付加情報は 7 バイトに限定されるものではない。

 packets 付加情報は、タイムスタンプまたは位置情報を含んでなくてもよい。その場合、packets 付加情報は、2 バイトとなる。

25 暗号化データに 7 バイトの packets 付加情報を付加すると、RTP プロトコルのペイロードが形成され、ヘッダとして RTP ヘッダが付加されると、RTP プ

ロトコルが形成される。

RTPプロトコルは、TCPパケットまたはUDPパケットのペイロードであり、ヘッダとして、TCPヘッダまたはUDPヘッダが付加されると、TCPパケットまたはUDPパケットが形成される。

5 TCPパケットまたはUDPパケットは、IPパケットのペイロードであり、ヘッダとしてIPヘッダが付加されると、IPパケットが生成される。

さらにこのIPパケットはMACフレームのペイロードであり、ヘッダとしてイーサネットヘッダが付加されると、イーサネットパケットが生成される。

10 イーサネット(R)ヘッダとしては、図10に示す様に、標準的なイーサネット(R)ヘッダとIEEE 802.1Q(VLAN)により拡張されたイーサネット(R)ヘッダのと両方が適用可能である。

標準的なイーサネットヘッダは14バイトであり、6バイトのDA(Destination Address)と、6バイトのSA(Source Address)と、2バイトで示される長さ/タイプを示す情報とを含む。

15 802.1Qで拡張されたイーサネットヘッダは18バイトあり、802.1Qで拡張されたイーサネットヘッダは、標準的なイーサネットヘッダと、SAと長さ/タイプを示す情報との間に4バイトの802.1q拡張部が設けられている点で異なる。

20 802.1q拡張部は、2バイトのTPID(Tag Control ID)と、VLAN優先度を示す2バイトのTCI(Tag Control Information)とを含む。

TCIは、3ビットのPriority(User Priority)と、1ビットのCFI(Canonical Format Indicator)と、12ビットのVID(VLAN Identifier)とを含む。

25 Priorityの使用法は、ISO/IEC 15802-3で規定されており、このPriorityのフラグを用いて、イーサネット(R)フレームの

優先度を設定することができる。

以上により、送信装置と受信装置との間で送信データ（例えば、MPEG-TS）を暗号化してリアルタイム伝送が可能となる。また、第2の packets 化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信 packets の送り残しや受信 packets の取りこぼしが発生しない。これにより、全ての優先データ packets が完全に送信され、リアルタイム性の保証された高品質映像の伝送が可能となる。

また、一般データは一時的にバッファに蓄積され、優先データの伝送が優先的に行なわれる間に間欠的に伝送される。また、処理すべきデータ量の小さい第1のパケット化手段はマイコンなど安価なプロセッサで構成してもよい。

さらに、ハードウェア処理により、受信処理においても、イーサネット（R）フレームを受信して、3層のIPヘッダ、4層のUDPヘッダを同時に検査することもできる。

また、優先データであるコンテンツデータ（例えば、MPEG-TS）のパケットと一般データのパケットとを分離し、コンテンツデータのパケットの処理をハードウェアで行うことにより、受信フレームの取りこぼしが発生せず、リアルタイム性が保証された高品質な受信を行うことができる。

パケットを送信するタイミング、または、2つのキュー手段からのパケットを送信する割合をソフトウェアではなくハードウェアで制御することによって、クロック単位で完全に送信を制御することが可能である。これにより全ての優先パケットが完全に送信され、リアルタイム性の保証された高品質の伝送が可能となる。また、出力パケットのシェイピングもクロック単位で正確に行われるため、初段のルータ、またはスイッチングハブでのパケット廃棄の発生確率が非常に少ない高品質な通信が可能となる。

(実施の形態 4)

図 1 1 は、本発明の実施の形態 4 によるパケット送受信装置 4 0 1 C のブロック図を示す。

AKE 手段 4 0 2 が、D T C P 情報生成手段 1 0 0 1 と、AKE コマンド受信処理手段 1 0 0 2 と、AKE コマンド送信処理手段 1 0 0 3 と、交換鍵生成手段 1 0 0 4 と、暗号化鍵生成手段 1 0 0 5 と、暗号化鍵変更情報生成手段 1 0 0 6 と、復号鍵生成手段 1 0 0 7 とを含む点を除いてパケット送受信装置 4 0 1 C は、実施の形態 4 において図 8 を参照して説明したパケット送受信装置 4 0 1 B と同様の構成である。したがって、以下の説明では、主に、D T C P 情報生成手段 1 0 0 1 と、AKE コマンド受信処理手段 1 0 0 2 と、AKE コマンド送信処理手段 1 0 0 3 と、交換鍵生成手段 1 0 0 4 と、暗号化鍵生成手段 1 0 0 5 と、暗号化鍵変更情報生成手段 1 0 0 6 と、復号鍵生成手段 1 0 0 7 とについて説明する。

パケット送受信装置 4 0 1 C においては、以下のステップに従った D T C P 方式により暗号化送信データの送信が行なわれる。ここでは、パケットを送信するソースおよびパケットを受信するシンクの両方の機能を、パケット送受信装置 4 0 1 C を参照して説明するが、これは、説明を簡略化するためであり、実際には、二つの異なるパケット送受信装置においてパケットの送受信が行われることに留意されたい。

(ステップ 1) 認証・鍵交換関連情報として、伝送時における暗号化送信データの暗号化状態を表すコピー保護情報が D T C P 情報生成手段 1 0 0 1 に入力される。

(ステップ 2) まず、送信装置 (ソース) においてデータの送信要求を発生させ、D T C P 情報生成手段 1 0 0 1 からデータの保護モード情報 (E M I 情報) が第 1 のパケット化手段 7 0 1 に出力され、送信パケットが生成され、送信パケットは送信装置から送信される。

(ステップ 3) 送信装置から送信された送信パケットは、受信装置 (シンク) において、受信パケットとして受信され、AKE コマンド受信処理手段 1 0 0 2

は、第1の packets 受信手段703から受け取ったデータのコピー保護情報を解析し、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、AKE送信処理手段1003を通じて認証要求を送信装置に送る。

(ステップ4) 送信装置と受信装置との間でD T C P方式の所定の処理が行なわれ、認証鍵が共有される。

(ステップ5) 次に、送信装置はAKE送信処理手段1003において、認証鍵を用いて交換鍵を暗号化することによって生成した暗号化交換鍵を第1の packets 化手段701を介して受信装置に送り、受信装置においてAKEコマンド受信処理手段1002によって暗号化交換鍵は抽出され、交換鍵生成手段1004において交換鍵に復号される。

(ステップ6) 送信装置では、暗号化鍵を時間的に変化させるために、暗号化鍵生成手段1005において、時間とともに変更するシード情報(O/E)を生成し、シード情報は、D T C P 情報生成手段1001および第1の packets 化手段701を介して受信装置に送信される。

(ステップ7) 送信装置では、暗号化鍵生成手段1005において交換鍵とシード情報とを用いて暗号化鍵を生成して、暗号化手段406は、この暗号化鍵を用いて、送信データ(例えば、M P E G - T S)を暗号化して、暗号化送信データを生成し、暗号化手段406は、暗号化送信データを第2の packets 化手段702に出力する。

(ステップ8) 受信装置では、暗号化鍵変更情報生成手段1006は第1の packets 受信手段703からシード情報を受信し、復号鍵生成手段1007はこのシード情報と交換鍵生成手段1004の交換鍵とを用いて、暗号化鍵(復号鍵)を生成する。

(ステップ9) 受信装置では、この暗号化鍵(復号鍵)を用いて復号手段407において、暗号化されたデータを復号する。

図12は、packets 化手段403に含まれる第1の packets 化手段701およ

び第2の packets 化手段702、ならびに、packets 受信手段405に含まれる第1の packets 受信手段703および第2の packets 受信手段704における packets 処理について説明するためのブロック図である。

第1の packets 化手段701では、入力されたデータを、R T C PまたはR T S Pプロトコル、T C PまたはU D Pプロトコル、さらにはI Pプロトコルに形成するための処理が順次なされる。

なお、R T C Pプロトコル(r f c 1 8 8 9)を使用する場合には、ネットワークの実効帯域幅および遅延時間などといったネットワークの通信状態を受信装置より送信装置に送り、送信装置は送られてきたネットワークの通信状態に合わせてR T Pで送信するデータの品質を調整して送信することもできる。

また、R T S Pプロトコル(r f c 2 3 2 6)は、再生、停止、早送りなどの制御コマンドを送ることもでき、A Vファイルからデータをダウンロードしながらデータを再生することが可能である。

第2の packets 化手段702では、入力されるデータをR T Pプロトコル、U D Pプロトコル、そして、I Pプロトコルに形成するための処理がそれぞれ順次行われ、I P packets が生成される。

また、第1の packets 受信手段703では、フィルタリングなどのI Pプロトコルの受信処理、T C PまたはU D Pプロトコルの受信処理、さらに、R T C PまたはR T S Pプロトコルの受信処理が順次行われ、それにより、受信 packets に含まれる受信データが抽出される。

また、第2の packets 受信手段704は、フィルタリングなどのI Pプロトコルの受信処理、U D Pプロトコルの受信処理、さらに、R T Pプロトコルの受信処理が順次なされ、受信 packets に含まれる受信データが抽出される。

以上により、送信装置と受信装置との間でデータ(例えば、M P E G - T S)をD T C P方式に基づいて暗号化し、リアルタイムな伝送が可能となる。また、第2の packets 化手段がハードウェアで構成されているため、本質的にソフトウ

エア処理に起因する送信パケットの送り残しおよび受信パケットの取りこぼしが発生しない。また、データ量の小さい第1のパケット化手段はマイコンなどの安価なプロセッサで構成することができる。

また、何らかの原因であらかじめ決められた条件に合致しないために受信装置と受信装置との認証が成立しない場合であっても、例えば、すでに送信装置または受信装置が記憶している証明書、MACアドレスなどの情報および指紋、虹彩などの個人を特定する生体情報の少なくとも1つを用いて、送信装置と受信装置との認証をおこなってもよい。

再び、図11を参照すると、認証・鍵交換手段402のAKEコマンド受信処理手段1002は、パケット送受信装置401Cと、送信パケットの到着先または受信パケットの送信元との間で認証を行った場合に、送信パケットの到着先または受信パケットの送信元に関する情報を一時的に記憶する記憶手段と、パケット送受信装置と、送信パケットの到着先または受信パケットの送信元とがあらかじめ決められた条件に合致しないために認証が成立しない場合に、記憶手段にて記憶された情報と、送信パケットの到着先に関する情報または受信パケットの送信先に関する情報とを照合し、パケット送受信装置と送信パケットの到着先または受信パケットの送信元との間で認証を行う、照合手段として機能してもよい。

これにより、例えば、家庭で相互認証を行った2つの機器を遠隔地間で特定認証可能となり、家庭と旅行先などの遠隔地との間でのデータコンテンツの伝送、データコンテンツのリモート伝送が可能となる。

(実施の形態5)

図13は、パケット化手段403Aの第1のパケット化手段701および第2のパケット化手段702A、ならびに、パケット受信手段405A内の第1のパケット受信手段703および第2のパケット受信手段704Aにおけるパケット処理について説明するためのブロック図である。

パケット化手段403Aおよびパケット受信手段405Aは、第2のパケット化手段702、および、第2のパケット受信手段704Aが異なる点を除いて、図12を参照して説明したパケット化手段403およびパケット受信手段405と同様の構成である。したがって、以下の説明では、主に第2のパケット化手段702A、および、第2のパケット受信手段704Aについて説明する。

第2のパケット化手段702Aは、入力されるデータに対してエラー訂正処理を行ない、RTPプロトコル、UDPプロトコル、そしてIPプロトコルを形成するようにそれぞれ順次的に処理することによって、IPパケットを生成する。

また、第2のパケット受信手段704Aは、フィルタリングなどのIPプロトコルの受信処理、UDPプロトコルの受信処理、RTPプロトコルの受信処理、さらにエラー訂正符号処理を順次的に行い、それにより、エラー訂正されたデータが出力される。

図14は、本発明の実施の形態5によるプロトコルスタックを説明するための模式図である。

送信装置では、AVデータにエラー訂正符号が付加され（ECCエンコード）、UDPプロトコルに渡される。また、受信装置では、UDPプロトコル処理よりデータを受け取りエラー訂正をして上位層のAVデータとなる。

エラー訂正方式の例を、図15および図16を参照して、以下に説明する。

図15は、エラー訂正方式がリードソロモン方式である場合を説明するための模式図である。

図16は、エラー訂正方式がパリティ方式である場合を説明するための模式図である。

ここでは、2つの単位のデータ（MPEG-TS）をエラー訂正インターリーブマトリックスに入力している。なお、各行にはシーケンス番号を2バイト使用している。

次いで、たとえば、2バイトのパケット付加情報を用いて、さらに、RTPへ

ッダ、UDPヘッダ、IPヘッダ、イーサネット（R）ヘッダを付加することによって、イーサネット（R）フレームを生成する。

このように、送信装置と受信装置との間でデータ（例えば、MPEG-TS）をDTC方式に基づいて暗号化し、さらにエラー訂正符号を付加して、リアルタイムに伝送することが可能となる。

また、第2の packets 化手段がハードウェアで構成されていると、本質的にソフトウェア処理に起因する送信パケットの送り残しおよび受信パケットの取りこぼしが発生しない。また、データ量の小さい第1の packets 化手段はマイコンなど安価なプロセッサで構成することができる。

（実施の形態6）

図17は、本発明の実施の形態6による packets 送受信装置401Dのブロック図である。

packets 送受信装置401Dでは、受信データ（例えば、MPEG-TSなどのAVデータ）の受信機能を取り除いた点を除いて、図11を参照して説明した packets 送受信装置401Cと同様の構成を有している。

図18は、本発明の実施の形態6の別の形態による packets 送受信装置401Eのブロック図である。

packets 送受信装置401Eは、送信データ（例えば、MPEG-TSなどのAVデータ）の送信機能を取り除いた点を除いて、図11を参照して説明した packets 送受信装置401Cと同様の構成を有している。

なお、このように、データの受信機能または送信機能を取り除くことは、実施の形態1から実施の形態5にて説明したすべての packets 送受信装置に適用できる。また、本発明は、送信または受信のみを行う機器に対しても適用可能であり、それにより、低コスト化を図ることができる。

なお、上述した実施の形態1から6においては、一般のIPネットワークなど

パケットの順序性が保証されていない通信網で伝送する場合には、シーケンス番号を付加したパケットを送信し、受信装置にてパケットに付加されたシーケンス番号を用いて順序性の保証を行ってもよい。この順序性の保証は、OSIモデルの第4層以上、すなわち、RTPプロトコルまたはビデオ信号処理などで行なうことができる。

なお、送信装置においてハードウェア処理され、伝送されたAVデータのパケットは、ネットワークにおいてフラグメント化されることを防ぐことができる。具体的には、送信装置において、あらかじめアプリケーションレベルの処理で、通信網においてフラグメント化されない最大サイズ(MTU)を検査し、それ以下のパケットサイズで伝送すればよい。

具体的には、送信条件設定管理手段404および受信条件設定管理手段408は、送信フレームの送信から到着するまでの間において送信パケットの送信先から受信先までの経路における最大伝送パケットサイズの検出を行ない、最大伝送パケットサイズ情報を用いて、送信条件設定情報または受信条件設定管理手段を生成してもよい。

あるいは、RFCの規格において、全ての端末は576バイトのサイズのIPパケットを取り扱えなければならないと規定されているので、ルータ等の多くのネットワーク機器ではこれ以下のIPパケットに対してフラグメント化が起らない。したがって、IPパケットのサイズが576バイト以下となるように、送信装置でハードウェア処理されるAVデータのパケットサイズを調整すればよい。なお、送信装置でハードウェア処理されるAVデータのパケットにフラグメント化が起らない場合は、受信したパケットがフラグメント化されていれば全て一般パケットとして処理すればよい。なお、イーサネット(R)のIPパケットの最大値を越えた場合は送信装置においてフラグメント化する必要がある。したがって、優先パケットのフラグメント化を起こさせないためにはIPパケットの最大値以下でなければならないことは言うまでもない。

また、通信網においてフラグメント化が起こる確率が非常に低い場合は、送信装置でハードウェア処理され伝送されたAVデータのパケットのIPヘッダにフラグメント禁止のフラグを付して伝送することにより、ルータがフラグメントせざるを得ない状態ではIPパケットを廃棄させることにより、受信装置のフラグメント化処理負荷を軽減してもよい。この場合、非常に少数のパケットは損失となるが、受信装置で誤り訂正あるいは誤り修整を行うことで通信品質を補償することができる。

さらに、実施の形態1から6においては、通信網プロトコルの具体例としてイーサネット(R)を説明したが、本発明は、これに限定されるものではない。

また、ビデオ信号処理の例として、実施の形態1から6ではMPEG-TSを用いたが、本発明は、これに限定されるものではない。本発明の入力ストリームは、MPEG1/2/4などMPEG-TSストリーム(ISO/IEC 13818)、DV(IEC 61834、IEC 61883)、SMPTE 314M(DV-based)、SMPTE 259M(SDI)、SMPTE 305M(SDTI)、SMPTE 292M(HD-SDI)等で規格化されているストリームを含んだあらゆる映像、音声に関するストリームまでも適用可能である。

映像または音声のデータレートは、CBR(constant bit rate)に限定されるものではない。VBR(variable bit rate)でもよい。さらに、映像または音声だけでなく、一般のリアルタイムデータ、あるいは優先的に送受信を行うデータであればどのようなものでも本発明から排除されるべきではない。

また、本発明で使用されるデータは、ファイルであってもよい。データがファイルである場合、送信装置と受信装置との間の伝播遅延時間と、送信装置および受信装置の処理能力との関係により、一定の条件下でリアルタイムよりも高速に伝送することも可能である。

また、インターネットの分野で一般にストリーミングと呼ばれているコンテンツ伝送方式も実現可能である。ストリーミング方式のコンテンツ伝送の場合、送信装置から受信装置のバッファにネットワークを介してTCP/IPまたはUDP/IPによりコンテンツデータを伝送し、受信装置のバッファからコンテンツデータを比較的一定のレートで読み出すことによって、受信装置において連続したデータを再生することができる。

また、本発明は、SMPTE (www. smpte. org) において規格化されたGXFファイルフォーマット (SMPTE 360M)、および、規格化が推進されているMXFファイルフォーマットに準拠したファイルの暗号化伝送にも適用可能である。

(実施の形態7)

実施の形態7について説明する。

図19は、本発明の実施の形態7によるパケット送信手段1101のブロック図である。

ここで、パケット送信手段1101は、図4を参照して説明したパケット送受信装置401のパケット化手段403およびフレーム化手段409に相当する。

パケット送信手段1101は、一般データ入力手段1102と、パケット化情報入力手段1104と、一般データパケット化手段1105と、バッファ手段1106と、有効データ抽出手段1107と、優先データパケット化手段1109と、パケット送信順序制御手段1113と、フレームデータ送信手段1114とを備える。

パケット送信手段1101において、優先データが優先データ入力手段1103から有効データ抽出手段1107に入力される。有効データ抽出手段1107は、入力された優先データから無効なデータ成分を取り除き、有効ペイロードを抽出して有効データ1108を優先データパケット化手段1109に入力する。

優先データパケット化手段 1 1 0 9 は、図 8 を参照して説明したパケット送受信装置 4 0 1 B の第 2 のパケット化手段 7 0 2 に相当する。

パケット送信順序制御手段 1 1 1 3 は、図 8 を参照して説明したパケット送受信装置 4 0 1 B の送信キュー制御手段 6 0 1 に相当する。

5 有効データ抽出手段 1 1 0 7 における処理内容としてはデータのバッファリング、データビット数変換、クロック周波数変換などを含む。

具体例としては、優先データのストリームとして SMPTE 3 2 1 M 規格の SDTI ストリームがあり、また、有効データとして SMPTE 3 1 4 M 規格の DIF データがある。

10 あるいは、優先データのストリームとして DVB、A 1 0 M 規格の DVB-A SI ストリームがあり、また、有効データとして MPEG 規格の MPEG-TS パケットがある。

優先データパケット化手段 1 1 0 9 は、パケット化情報と、有効データ 1 1 0 8 を用いて、優先データパケットを生成する。

15 図 2 0 は、優先データパケットのプロトコルスタックを説明するための模式図である。

図 2 0 に示した AV データは、本実施の形態において、優先データ入力手段 1 1 0 3 から入力される優先データである。

20 図 2 0 に示したように AV データを処理することによって、イーサネット (R) フレームが生成される。

一方、一般データ入力手段 1 1 0 2 は、一般データが入力される。一般データは、一般的に、必ずしもリアルタイムで送る必要の無いデータである。一般化データパケット化手段 1 1 0 5 は、一般データを用いて一般データパケットを生成し、一般データパケットを出力する。なお、一般データ入力手段 1 1 0 2 はデータのインタフェースを行うものである。

一般化データパケット化手段 1 1 0 5 は、図 8 を参照して説明したパケット送

受信装置 4 0 1 B の第 1 のパケット化手段 7 0 1 に対応する。

一般データの例としては、前述した機器の動作制御に関する情報、SNMP および MIB 等の管理情報があり、これらは TCP/IP あるいは UDP/IP を用いて伝送される。

5 一般データパケット化手段 1 1 0 5 から出力される一般データパケットは、バッファ手段 1 1 0 6 に入力され、バッファ手段 1 1 0 6 は一般データパケットを一時的に蓄積する。ここで、バッファ手段 1 1 0 6 に一般データパケットが蓄積されると、バッファ手段 1 1 0 6 はパケット送信順序制御手段 1 1 1 3 に送信要求信号 1 1 1 0 を通知（アサート）して送信要求を行う。

10 一般的に、ビデオデータなどのコンテンツデータをリアルタイムでストリーム伝送するためには、リアルタイム性を必要としないデータよりもビデオデータを優先的に処理する必要がある。

15 パケット送信順序制御手段 1 1 1 3 は、優先データパケットの送信を優先させつつ、送信要求信号 1 1 1 0 がアサートされた場合には、優先データパケットのリアルタイム性を損なわない範囲で一般データパケット 1 1 1 2 の送信を許可する。送信許可は、バッファ手段 1 1 0 6 に対する送信許可信号 1 1 1 1 をアサートすることにより、バッファ手段 1 1 0 6 から一般データパケットを送信することを許可する。

20 フレームデータ送信手段 1 1 1 4 は、パケット送信順序制御手段 1 1 1 3 から入力された送信パケットを用いて、イーサネット（R）フレームを生成し、送信フレームとしてネットワークに出力する。

図 2 1 は、本実施の形態における送信タイミングチャートを説明するための模式図である。このタイミングチャートに例示する方式は、本実施の形態の要点の 1 つである優先データパケットと非優先データパケット（一般データパケット）
25 の送信制御方式である。

図 2 1 では、送信パケット 2 1 0 3 の送信開始タイミング 2 1 0 1 と、送信要

求信号 1 1 1 0 のパルス波形 2 1 0 2 と、送信パケット 2 1 0 3 とを時間的に対応するように示している。

送信開始タイミング 2 1 0 1 では、優先データパケットを含む送信フレームが送信されるタイミングを上向き矢印で示し、非優先データパケットを含む送信フレームが送信可能なタイミングを下向き矢印で示している。

また、送信パケット 2 1 0 3 は優先データパケットを白抜き、非優先データパケットを黒塗りで示している。

本実施の形態では、一例として以下のような優先データを送信する場合を例として説明する。優先データが、DVCPRO 25 (SMPTE 314M で規定) である場合、NTSC モードでは 1 フレーム期間に 1 2 0, 0 0 0 バイトのデータが発生するので、データレートは約 5 7. 6 メガビット/秒 (約 5 7. 6 Mbps) の一定レート (CBR) となる。ここでは、AV データのビデオペイロード長を 1 2 0 0 バイト、システムクロックは 2 7 MHz としている。

優先データである AV データのパケット発生率は、 $1\,200\,000 / 1\,200 = 1\,000$ パケット/フレーム = 2 9 9 7 パケット/秒となる。

したがって、優先データパケットのみを伝送する場合であれば、 $2\,700\,000 / 2\,997 = 9009.9$ クロックに一回パケットを送信すればよい。つまり 9 0 0 9. 9 クロックが平均送信間隔である。

本実施の形態によれば、この平均送信間隔より短い間隔で優先データパケットを送信することにより、非優先データパケットを送信するタイミング余裕 (送信余裕期間) を創り出している。

具体的には、優先データパケットの送信間隔を 8 1 0 0 クロックとし、優先データパケット 9 回毎に 1 回、非優先データパケットの送信を許可可能な送信余裕期間を創り出す。9 0 0 9. 9 クロックで 9 個の優先パケットを送信する場合は $9009.9 * 9 = 81089.1$ クロックを要する。ここでは議論を簡単にするため、平均値で検討する。ただし、小数点以下の数値も用いている。

本実施の形態では9009.9クロックよりも短い8100クロックで送信するので、実際には、 $8100 \times 9 = 72900$ クロックが必要である。

したがって非優先データパケットを送信する送信余裕期間は81089.1-72900=8189.1クロックである。

5 送信開始タイミング2001において、優先データパケットを送信するタイミングを示す上向き矢印から次の矢印までの間隔は8100クロックである。9回の優先パケット送信タイミングに1回、非優先パケットの送信タイミングが現れる(2104、2105、2106)。非優先パケットの送信タイミングを示す下向き矢印から次の矢印までの間隔は8189クロックである。

10 パルス波形2102に示されるように、送信要求信号1110はバッファ手段1106に、送信すべき一般データが蓄積されると、送信要求信号をアサートする。図21においてはパルス波形2102がHighになる。

15 パルス波形2102において、送信要求信号1110がタイミング2107のいてHighになり、次に、送信開始タイミング2101において、一般データパケットの送信可能タイミングになったタイミング(タイミング2108)で送信許可信号1111がアサートされ(図21には図示せず)、一般データパケット2111が送信される。一般データパケットが送信開始されたタイミングで送信要求信号1110はデアサートされる(パルス波形2102のタイミング2108)。

20 タイミング2105では、送信要求信号1110がアサートされていないので送信すべき一般データパケットはバッファ手段106には存在せず、タイミング2105において一般データパケットは送信されない。

25 つぎにタイミング2109で送信要求信号1110のパルス波形2102が再びアサートされ、タイミング2110で一般データパケット2112が送信される。送信要求信号1110は一般データパケット2112が送信開始されるとデアサートされる(パルス波形2102のタイミング2110)。

なお、バッファ手段 1106 に複数の一般データパケットが蓄積されている場合は、一つの一般データパケットが送信されても、送信要求信号 1110 はデアサートされず、残りの一般データパケットは次の一般データパケットの送信可能タイミングを待って、1 パケットずつ送信される。このようにして優先データパケットが優先的に送信される。

送信パケットは、上記のようにパケット送信順序制御手段 1113 からフレームデータ送信手段 1114 に出力される。フレームデータ送信手段 1114 は、入力された送信パケットを用いて、物理層とのインタフェースが可能なイーサネット (R) フレームを生成し、送信フレームとして転送する。なお、10Mbps および 100Mbps のイーサネット (R) では IEEE 標準インタフェースが規定されており、ギガビットイーサネット (R) では IEEE 標準インタフェースが規定されている。

なお、本実施の形態では、優先データパケットと一般データパケットの送信制御をクロック単位でそれぞれのパケットに割り当てる時間を決めたが、本発明は、これに限定されない。本発明は、例えば、優先データパケット化手段 1109 のバッファに一定量の優先データパケットを格納し、優先データパケットの平均パケット生成量よりも短い時間間隔でパケット送信順序制御手段 1113 で優先的に送信を行い、バッファでの優先パケットの格納量が、あるスレッシュホールドレベル以下になったときに一般データパケットに送信を割り当てるなどとしてもよい。

以上のように、本実施の形態では優先データから有効データを抜き出し、優先データパケットとして一般データパケットよりも優先して送信することが可能である。

図 22 は、本発明の実施の形態 7 の変形例によるパケット送信手段 1101A を示すブロック図である。

パケット送信手段 1101A は、有効データ抽出手段 1107 から、優先データのフォーマットに関する情報を示す優先データフォーマット情報を優先データ

フォーマット情報出力手段 1201 を介して外部に出力する点を除いて、図 19 を参照して説明したパケット送信手段 1101 と同様の構成を有している。したがって、以下の説明では、主に、優先データフォーマット情報出力手段 1201 について説明する。

- 5 パケット送信手段 1101 A において、出力される優先データのフォーマット情報を用いて外部のコンピュータ等で優先データのパケット化情報を設定すると、効率的にパケットの送信を行うことができる。

(実施の形態 8)

- 10 実施の形態 8 について説明する。

図 23 は、本発明の実施の形態 8 によるパケット送信手段 1101 B のブロック図である。

- 15 パケット送信手段 1101 B は、優先データパケット化情報生成ブロック 1301 を含み、有効データ抽出手段 1107 から、優先データフォーマット情報を優先データパケット化情報生成ブロック 1301 に出力する点を除いて、図 19 を参照して説明したパケット送信手段 1101 と同様の構成を有している。したがって、以下の説明では、主に、優先データパケット化情報生成ブロック 1301 について説明する。

- 20 優先データパケット化情報生成ブロック 1301 にはパケット化情報が入力され、優先データパケット化情報生成ブロック 1301 は、パケット化情報と優先データフォーマット情報とを用いて、優先データのパケット化情報を更に最適に設定しなおす。これにより、外部においてパケット化情報をラフに生成した場合でも最適なパケット化情報を生成できるため、より効率的にパケットを送信することができる。

- 25 本実施の形態によれば、有効データ抽出手段 1107 から優先データフォーマット情報を得て、外部から入力されるパケット化情報と共にパケット化パラメー

タの決定に使用することができる。これにより、たとえば、優先データがDV系の場合はD I Fブロックの80バイト単位、また、M P E G系の場合はT Sパケットの188バイト単位で優先データのパケット化を自動的に行うことができる。

図24は、本発明の実施の形態8の変形例によるパケット送信手段1101Cのブロック図である。

パケット送信手段1101Cは、MTU (Maximum Transfer Unit) サイズ入力手段1401を設けた点を除いて、図23を参照して説明したパケット送信手段1101Bと同様の構成を有している。したがって、以下の説明では、主に、MTUサイズ入力手段1401について説明する。

パケット送信手段1101Cでは、MTUサイズ（最大伝送サイズ）がMTUサイズ入力手段1401から入力される。MTUサイズは伝送路における優先データの最大伝送パケットサイズを意味する。優先データパケット化情報生成ブロック1301は、優先データパケット化手段1109にて生成される優先データパケットのサイズが入力されるMTUサイズ以下になるようにパケット化情報1402を生成する。これにより、優先データ送信におけるフラグメント化を防止でき、安定して優先データを通信することが実現できる。

（実施の形態9）

実施の形態9について説明する。

図25は、本発明の実施の形態9による優先データパケット化手段1109のブロック図である。

優先データパケット化手段1109は、実施の形態2において図8を参照して説明された第2のパケット手段702に含まれている。

優先データパケット化手段1109は、バッファ手段1501と、バッファ手段1501と、パケットヘッダ生成手段1503と、パケット合成手段1504とを含む。

優先データパケット化手段 1109 において、有効データ 1108 がバッファ手段 1501 およびカウンタ手段 1502 に入力される。有効データ 1108 は、クロック信号とデータとデータ有効フラグとを含む。

5 バッファ手段 1501 は、有効データ 1108 のデータ有効フラグがアサート（有効）されている時と時のみデータを蓄積する。

また、カウンタ手段 1502 も、同様に有効データ 1108 のデータ量をカウントして内部のレジスタに保持する。

10 一方、パケット化情報 1104（1302、1402）がパケットヘッダ生成手段 1503 に入力され、ここで、UDP/IP パケットヘッダが生成されパケット合成手段 1504 に入力される。また、パケットヘッダ生成手段 1503 から、パケット（例えば、IP パケット）のペイロード長がカウンタ 1502 に出力され、カウンタ手段 1502 からこのペイロード長分の優先データを読み出すための制御信号がバッファ手段 1501 に送られる。

15 これによりバッファ手段 1501 は、パケットヘッダ生成手段 1503 により指定されたペイロード長の優先データをパケット合成手段 1504 に出力する。パケット合成手段 1504 は、パケットヘッダ生成手段 1503 にて生成された UDP/IP パケットヘッダと、指定されたペイロード長の優先データとを合成して UDP/IP パケットを生成し、出力手段 1505 から出力する。

20 図 26 は、本発明の実施の形態 9 の変形例による優先データパケット化手段 1109A のブロック図である。

25 優先データパケット化手段 1109A は、カウンタ手段 1502 からパケットヘッダ生成手段 1503 に優先データパケットのペイロード長を示す情報が入力される経路 1601 が設けられている点を除いて、図 25 を参照して説明した優先データパケット化手段 1109 と同様の構成を有している。したがって、以下の説明では、主に、この経路 1601 について説明する。

優先データパケット化手段 1109A において、カウンタ手段 1502 より優

先データパケットのペイロード長を示す情報がパケットヘッダ生成手段 1503 にこの経路 1601 を介して入力される。パケットヘッダ生成合成手段 1503 は入力されたパケット化情報 1104 (1302、1402) とパケットペイロード長とを用いてパケットヘッダを決定する。

5 図 27 は、本発明の実施の形態 9 の別の変形例による優先データパケット化手段 1109B のブロック図である。

優先データパケット化手段 1109B は、エラー訂正付加手段 1701 がさらに設けられている点を除いて、図 26 を参照して説明した優先データパケット化手段 1109A と同様の構成を有している。したがって、以下の説明では、主に、
10 エラー訂正付加手段 1701 について説明する。

優先データパケット化手段 1109B において、バッファ手段 1501 より優先データパケットのペイロードがエラー訂正付加手段 1701 に入力される。エラー訂正付加手段 1701 では後述するパリティ付加方式またはリードソロモン方式により、エラー訂正符号を付加して生成されたパケットをパケット合成手段
15 1504 に入力する。

なお、優先データパケットの例としては、図 20 に示したように 1 次元で表現された AV データを用いてもよいが、AV データとして 2 次元的なマトリックスデータを利用することもできる。

20 図 28 は、エラー訂正がリードソロモン方式の場合のパケット構成を示す図である。

図 28 に示すように、縦方向 m 行 (m は整数で、例えば図 28 では 48 行) と横方向 n 列 (n は整数で、例えば図 28 では 1200 バイト) のマトリックス上にバイト単位 (8 ビット単位) で配置された AV データマトリックスにリードソロモン形式のエラー訂正を行い、4 行分の誤り訂正データを付加したデータマトリックスを (横 1200 バイト、縦 52 行) を生成し、データマトリックスの 1
25 行ずつを読み出し、シーケンス番号または信号フォーマット情報などをヘッダ情

報として付加したデータを優先データパケットとしてもよい。

図 29 は、エラー訂正がパリティ処理方式の場合のパケット構成を示す図である。

AVデータとしては、縦方向 m 行（ m は整数で、例えば図 29 では 8 行）と横方向 n 列（ n は整数で、例えば図 29 では 1200 バイト）のマトリックス上にバイト単位（8 ビット単位）で配置された AV データマトリックスに縦の列方向にパリティ計算をして、1 行分のパリティデータを付加したデータマトリックスを生成し、前記データマトリックスの 1 行ずつを読み出し、シーケンス番号や信号フォーマット情報などをヘッダ情報として付加したデータを優先データパケットとしてもよい。

さらに、優先データパケットを生成する別のマトリックス単位の例として、縦方向 m 行（ m は整数で、例えば 15）と横方向 n 列（ n は整数で、例えば 80）のマトリックスを k 個（ k は整数で、例えば 5）生成し、まず k 個のマトリックスの同じ行にまず 1 行ずつデータを埋め込んでいくいわゆる k 個のマトリックにおける行単位のデータインターリーブ処理を行ない、ある m 行 n 列のマトリックデータが埋まった時点でマトリックスに縦の列方向にパリティ計算をして、1 行分のパリティデータを付加したデータマトリックスを生成し、前記 k 個のデータマトリックスの 1 行目のデータを k 個読み出し、次に前記 k 個のデータマトリックスの 2 行目のデータを k 個読み出すという順番で、前記 k 個のデータマトリックスの m 行目のデータを k 個読み出し、これらそれぞれにシーケンス番号や信号フォーマット情報などをヘッダ情報として付加したデータを優先データパケットとしてもよい。

以上のように、送信装置内の優先データパケット化手段において、優先データにエラー訂正符号を付加することにより、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データを復元することが可能になる。

(実施の形態 10)

実施の形態 10 について説明する。

図 30 は、本発明の実施の形態 10 によるパケット送信手段 1101D のブロック図である。

5 パケット送信手段 1101D は、暗号化情報入力手段 1011 および優先データパケット化手段 1109C における暗号化情報入力手段 1012 を設けた点を除いて、図 23 を参照して説明したパケット送信手段 1101B と同様の構成を有している。

10 図 31 は、本発明の実施の形態 10 による優先データパケット化手段 1109C のブロック図である。

優先データパケット化手段 1109C は、暗号化情報入力手段 1012 および暗号化手段 1122 が設けられた点を除いて、図 27 を参照して説明した優先データパケット化手段 1109B と同様の構成を有している。

15 したがって、以下の説明では、主に、暗号化情報入力手段 1011、優先データパケット化手段 1109C における暗号化情報入力手段 1012 および暗号化手段 1122 について説明する。

暗号化手段 1122 は、図 4 を参照して説明したパケット送受信装置 401 の暗号化手段 406 に相当している。

20 パケット送信手段 1101D において、暗号化情報が暗号化情報入力手段 1011 から、優先データパケット化手段 1109C における暗号化情報入力手段 1012 に入力される。

25 優先データパケット化手段 1109C において、バッファ手段 1501 から出力されたデータは、暗号化手段 1122 に入力され、暗号化情報入力手段 1011 から入力される暗号化情報を用いて暗号化される。暗号化手段 1122 で暗号化されたデータはエラー訂正付加手段 1701 に入力される。

なお、暗号化を行うために使用される情報は、送信装置の独自情報（機器 ID、

機器の認証情報、マックアドレスなど)、秘密鍵、公開鍵の少なくとも1つを用いて生成した情報であり、暗号化強度の強い暗号化方式と組み合わせることにより優先データパケットに対する強固な著作権保護を提供できる。

暗号化方式に関しては、たとえば、DTCP (Digital Transmission Content Protection) で使用されている暗号鍵Kcを適用することができる。なお、暗号鍵Kcの生成には、送信装置および受信装置でDTCP方式に基づいた認証処理を行なえばよい。この処理は公知の技術であり、たとえば、DTLA (Digital Transmission Licencing Administrator) (HYPERLINK "http://www.dtcp.com/" http://www.dtcp.com/, http://www.dtcp.com/data/dtcp_tut.pdf) や、書籍「IEEE1394、AV機器への応用」、高田信司監修、日刊工業新聞社、「第8章、コピープロテクション」、133～149ページにおいて説明されている。また、機器の認証情報は、公的または私的な認証機関でネットワーク等を介して適宜認証された証明情報を使用することができる。たとえば、政府認証基盤 (HYPERLINK "http://www.gpki.go.jp/" http://www.gpki.go.jp/) を参照することができる。

以上により、送信装置内の優先データのUDP/IPパケット伝送に際して、優先データを暗号化した後、エラー訂正を付加することによって、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データが復元可能になるとともに、ネットワーク上でのデータ盗聴、改竄を防止し、著作権が保護された安全性の高いAVデータ伝送を実現する。

(実施の形態11)

実施の形態11について説明する。

図 3 2 は、本発明の実施の形態 1 1 による優先データパケット化手段 1 1 0 9 D のブロック図である。

優先データパケット化手段 1 1 0 9 D において、暗号化情報切替手段 1 2 2 1 が設けられた点を除いては、図 3 1 を参照して説明した優先データパケット化手段 1 1 0 9 C と同様の構成を有している。したがって、以下の説明では、主に、

優先データパケット化手段 1 1 0 9 D において、時間的に変化する暗号化情報が暗号化情報入力手段 1 0 1 2 を介して暗号化切替手段 1 2 2 1 に入力され、暗号化切替手段 1 2 2 1 は、暗号化手段 1 1 2 2 で使用される暗号化情報を切り替える。

暗号化情報の切り替えタイミングの一例としては、エラー訂正付加手段 1 7 0 1 から得られる、エラー訂正マトリックス単位で切り替えるタイミングを使用することができる。これにより送信装置と受信装置との間で行う通信の暗号化強度をさらに強化しつつも、暗号の復号を着実に実現することができる。

優先データパケット化手段 1 1 0 9 D のバッファ手段 1 5 0 1 および暗号化手段 1 1 2 2 は、図 8 を参照して説明したパケット送受信装置 4 0 1 B の暗号化手段 4 0 6 に相当する。優先データパケット化手段 1 1 0 9 D のカウンタ手段 1 5 0 2、パケットヘッダ生成手段 1 2 0 3 および暗号化情報切替手段 1 2 2 1 は、図 8 を参照して説明したパケット送受信装置 4 0 1 B の A K E 手段 4 0 2 の一部および送信条件設定管理手段 4 0 4 の一部に相当する。優先データパケット化手段 1 1 0 9 D のパケットヘッダ生成手段 1 2 0 3 およびエラー訂正付加手段 1 7 0 1 は、図 8 を参照して説明したパケット送受信装置 4 0 1 B の送信条件設定管理手段 4 0 4、第 2 のパケット化手段 7 0 2 および暗号化手段 4 0 6 の一部に相当する。特に、優先データパケット化手段 1 1 0 9 D のエラー訂正付加手段 7 0 1 は、図 1 3 を参照して説明した第 2 のパケット化手段 7 0 2 A のエラー訂正符号付加手段に相当している。

図 3 3 は暗号の切り替えタイミングを説明するための模式図である。

図 3 3 に示されるように、暗号化情報切替手段 1 2 2 1 へ入力される暗号化情報は、エラー訂正マトリックスの切り替え時に切り替えられる。

暗号鍵切替に用いるタイミングとしては、エラー訂正マトリックスの終点または始点に同期して発生したタイミングである。

以上のように、エラー訂正マトリックスの位相を暗号鍵の切替位相とすることにより、暗号化強度を上げながら、暗号の復号をスムーズに実行することが可能となる。

なお、暗号鍵の切替位相としては、パケットヘッダ内に定義されたシーケンス番号の特定な値を使用してもよい。たとえば、エラー訂正が無い場合、シーケンス番号を 0 から 6 3 までの整数とし、シーケンス番号が 6 3 から 0 に更新されるタイミングを暗号鍵の切替位相として用いることができる。

また、暗号鍵切替手段 1 2 2 1 へ入力される暗号鍵を指定されたタイミングで切り替えながら暗号化手段 1 1 2 2 へ入力し、暗号化手段 1 1 2 2 における暗号化鍵を指定の間隔で切替えてもよい。

また、UDP/IP 以外のプロトコル、たとえば TCP/IP でパケットを送る場合にも、TCP ヘッダ内に含まれる TCP セグメントのシーケンス番号を用いることができる。なお、TCP プロトコルは IETF, RFC 793 で規定されている。

(実施の形態 1 2)

実施の形態 1 2 について説明する。

図 3 4 は、本発明の実施の形態 1 2 による優先データパケット化手段 1 1 0 9 E のブロック図である。

優先データパケット化手段 1 1 0 9 E において、フォーマットとポート番号との対応テーブル 1 4 0 1 が設けられた点を除いては、図 3 2 を参照して説明した

優先データパケット化手段 1109Dと同様の構成を有している。したがって、以下の説明では、主に、フォーマットとポート番号との対応テーブル 1401 について説明する。

優先データパケット化手段 1109Eにおいて、パケットヘッダ生成手段 1203は、上述した機能に加えて、さらに優先データフォーマット情報をUDPポート番号と対応させる。なお、優先データフォーマット情報はパケット化情報 1104に含まれている。

フォーマットとポート番号との対応テーブル 1401 には、優先データが使用するフォーマット情報が格納されており、入力されるパケット化情報 1104 内のフォーマット情報よりUDPポート番号が決定される。パケットヘッダ生成手段 1203は、このUDPポート情報を用いてUDP/IPパケットを生成する。

これにより、受信装置においてポート番号を検出するだけでフォーマット検出ができるため、受信装置での信号処理を簡単にすることが可能となる。また、2系統のストリーム処理が可能な受信装置で2つのストリームを同時受信している場合でもポート番号でフォーマットまたはチャンネルの識別が可能となる。

(実施の形態 13)

実施の形態 13 について説明する。

図 35 は、本発明の実施の形態 13 による、IEEE 1394 ストリーム伝送に適用したパケット送信システム 2000 のブロック図である。パケット送信システム 2000 は、実施の形態 1 において図 4 を参照して説明したパケット送受信装置 401 に含まれている。

パケット送信システム 2000 において、分離手段 1552 は、IEEE 1394 ストリームから一般データと、優先データとを分離する。ここで、一般データは、AV/C コマンドなどのアシンクロナス信号であり、また、優先データは、アイソクロナス信号である。

図36は、本発明の実施の形態13による、SDI/SDTI/DVB-ASIストリームの伝送に適用したパケット送信システム2500を示すブロック図である。

パケット送信システム2500において、RS232C、RRS422などから入力される制御、管理用信号は一般データとして、また、SDI/SDTI/DVB-ASIストリームから分離されたデータは優先データとして使用される。

図37は、本発明の実施の形態13によるパケット送受信装置1101Eのブロック図である。

このパケット送受信装置1101Eには、図19を参照して説明した実施の形態7によるパケット送信手段1101を適用している。

送信動作は上述の実施の形態7から13に記載した動作と同様である。受信処理としては、受信フレームから一般データパケットと優先データパケットとを分離し、それぞれから一般データと優先データを復号し出力する。

なお、上述した実施の形態7から13においては、パケットの順序性が保証されていない通信網で伝送する場合には、受信装置でパケットに付加されたシーケンス番号を用いて順序性の保証を行ってもよい。あるいは、後段のビデオ信号処理で順序性の保証を行ってもよい。

なお、受信側において優先パケットのフラグメント処理を行いたくない場合は、送信側において、あらかじめアプリケーションレベルの処理で、通信網においてフラグメントされない最大サイズ(MTU)を検査し、それ以下のパケットサイズで伝送すればよい。あるいは、RFCの規格では全ての端末は576バイトのサイズのIPパケットを扱えなければならないと規定されているので、ルータ等の多くのネットワーク機器はこれ以下のIPパケットではフラグメントが起らない。したがってIPパケットのサイズが576バイト以下となるように優先パケットを生成するようにすればよい。上記のように優先パケットにフラグメントが起らない場合は、受信したパケットがフラグメントされていれば全て一般パ

ケットとして処理すればよい。なお、イーサネット（R）のIPパケットの最大値を越えた場合は送信端末でフラグメントしなければ行けないので、優先パケットのフラグメントを起こさせないためにはIPパケットの最大値以下でなければならないことは言うまでもない。

5 また、通信網においてフラグメントが起こる確率が非常に低い場合は、送信側で優先パケットのIPパケットのIPヘッダにフラグメント禁止のフラグを立てて伝送することにより、ルータがフラグメントせざるを得ない状態ではIPパケットを廃棄させることにより、受信端末のフラグメント処理負荷を軽減してもよい。この場合、非常に少数の優先パケットは損失となるが、受信側で誤り訂正あ
10 るいは誤り修整を行うことで通信品質を補償することができる。

さらに、実施の形態7から13までは、通信網プロトコルとしてイーサネット（R）を例としたがこの限りではない。

また、ビデオ信号処理の例として、画像圧縮および伸張が行われるとしたが、圧縮されない場合でも本願発明の範囲から排除するものではない。また、あらか
15 じめMPEG等の方式で画像圧縮されたデータが入力される場合でも本願発明の範囲から排除するものではない。

また、ビデオではなく、オーディオ等のリアルタイムデータあるいは優先的に送受信を行うものであればどのようなものでも本発明から排除するものではない。

また、実施の形態7から13までは、CBR（constant bit rate）のビデオ信号を例としたが、優先データはCBRに限るものではない。
20

また、優先パケットはハードウェア処理、一般パケットはCPU処理としたが、処理スピードが間に合うのであればこの限りではない。

なお、上記説明は、当業者が、本発明を行い、または本発明を使用できるように提供される。これらの実施形態への様々な改変は、当業者に容易に明らかであり、本明細書中に明確にされる包括的原理は、さらなる発明の使用なしに他の実施形態に適用され得る。従って、本発明は、本明細書中に示される実施形態に限
25

定される意図はなく、本明細書中に開示される原理および新規な特徴と一致する最も広い範囲に合致されることを意図するものである。

産業上の利用可能性

5 本発明によれば、パケット送受信装置は、送信データのセキュリティを確保するためのAKE手段と、送信データの暗号化手段、AKE情報または送信制御情報を暗号化されたデータに付加するためのパケット付加情報生成手段、受信パケットからAKE情報または送信制御情報などの付加情報を抽出する手段、暗号化されたデータの復号手段と、送信パケットの送信先からフィードバックされるパ
10 ケット受信状況に基づいて適切なパケット送信条件を設定する送信条件設定管理手段と、パケット化手段と、パケット受信手段と、受信条件の設定管理手段とを備える。

これにより、DTCP方式をインターネットの標準プロトコルであるIPプロトコルに実装することができる。また、MPEG-TSなどのAVデータストリー
15 ムを送信装置で暗号化してデータの機密性および著作権の保護などを図りながら、パケット（例えば、IPパケット）をネットワークを介して伝送し、受信装置で元の信号に復号することが可能である。

本発明のある実施の形態によれば、パケット送受信手段は、送信パケットを一般パケットと優先送信されるパケットにクラス分けし、一般パケットを第1のデータキュー手段に、また、優先送信されるパケットを第2のデータキュー手段に入力する。そして、送信キュー制御手段により第1のデータキュー手段および第
20 2のデータキュー手段に一時的に蓄積されているパケットの送信順序を制御する。

これにより、データの機密性および著作権の保護を図りながら、リアルタイム性の高いデータを優先的に伝送することができる。また、入力ストリームが2チャンネル以上の複数ストリームの場合にも、それぞれのストリームに関する信号を
25 優先データと一般データにクラス分けすることにより対応が可能である。

本発明のある実施の形態によれば、パケット化手段は、第1のパケット化手段と第2のパケット化手段とを含む。ここで、AKE設定に関するAKE関連情報などの一般データは第1のパケット化手段に入力される。また、暗号化手段にて生成された暗号化送信データおよびAKE関連情報はハードウェアによるパケット化が実行される第2のパケット化手段に入力される。なお、AKE関連情報とは、コピー制御情報および暗号化鍵の更新情報のことである。第1のパケット化手段の出力は第1のデータキュー手段に入力され、第2のパケット化手段の出力は第2のデータキュー手段に入力される。送信条件設定管理手段から送信キュー制御手段に対して、第2データキュー手段に一時的に蓄積されている信号を優先的に出力するためのコマンドを出すと、暗号化されたデータが優先的に出力される。

このように第2のキュー手段がオーバフローしないように制御すれば、受信装置で適切な大きさのバッファを有しているため、送信装置と受信装置との間でデータコンテンツのリアルタイム伝送が実現できる。送信装置と受信装置との間でデータを暗号化してリアルタイム伝送する際に、第2のパケット化手段がハードウェアで構成されているため、ソフトウェア処理が間に合わないために発生する送信パケットの送り残しおよび受信パケットの取りこぼしといった不具合が発生しない。また、データ量の小さい第1のパケット化手段は安価なマイコンなどでも構成できるため、低コスト化が図れる。

本発明のある実施の形態によれば、パケット送受信手段は、AKE手段はDTCP方式で規定されている処理手順に準拠し、暗号化鍵生成手段と、DTCP情報生成手段と、AKEコマンド送信処理手段と、AKEコマンド受信処理手段と、交換鍵生成手段と、暗号化鍵変更情報生成手段と、復号鍵生成手段とを備える。暗号化鍵生成手段は、暗号化鍵を生成し、生成した暗号化鍵を暗号化手段に入力し暗号化動作を設定する。また、AKE情報生成手段は、外部から入力されるコピー制御情報、および、暗号化鍵生成手段から入力される鍵更新情報とを用いて

AKE関連情報を生成する。AKEコマンド送信処理手段は、暗号化鍵生成手段より暗号化鍵を、外部よりAKEパラメータを、さらにAKEコマンド受信処理手段よりAKEコマンド情報を受け取り、AKE送信コマンドを生成して、出力する。AKEコマンド受信処理手段は、第1の packets 受信手段よりAKE設定
5 制御情報を受け取り、AKE送信処理手段、交換鍵生成手段、暗号化鍵変更情報生成手段にそれぞれ設定制御情報を出力する。暗号化鍵変更情報生成手段は、AKEコマンド受信処理手段と第1の packets 受信手段からの情報を用いて暗号化鍵変更情報を生成する。復号鍵生成手段は、交換鍵生成手段と暗号化鍵変更情報生成手段からの情報を用いて、復号鍵を生成し復号手段に出力する。

10 これにより、D T C P方式に準拠したAKE手段を用いて、M P E P - T SなどのAVデータストリームを暗号化してリアルタイムに伝送することが可能となり、データの著作権保護を図ることができる。

本発明のある実施の形態によれば、 packets 送受信手段は、暗号化手段にて生成された暗号化送信データおよびAKE関連情報（例えば、コピー制御情報や暗
15 号化鍵の更新情報）が入力される第2の packets 化手段が、内部にエラー訂正符号付加手段を備えており、それにより、エラー訂正符号を付加される。

これにより、I Pネットワークで packets ロスまたはビットエラーなどが発生した場合にも受信装置でエラー訂正により送信データの復元が可能となる。また、第2の packets 化手段、および第2の packets 受信手段をハードウェアで構成
20 することが容易となる。

また、本発明のある実施の形態によれば、ネットワークを用いたAVコンテンツの伝送に関して、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した
25 場合においても、リアルタイム伝送される優先データ（AVデータ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるAVデータの販売、課金が可能となり、安全性の高いB - B、B - Cのコンテンツ販売流通が

可能となる。

また、本発明のある実施形態によれば、A Vコンテンツをハードウェアで伝送処理する場合にも、一般データパケットは従来通りC P Uを用いてソフトウェア処理を行う。よって、ソフトウェアの追加により管理情報や制御情報などデータを一般データとして伝送させることができる。これらのデータ量は優先データ量に比べて非常に少ないので、マイコンなど安価なマイクロプロセッサで実現可能となり低コストなシステムを実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価なC P Uや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できる。

また、本発明のある実施の形態においては、優先して送信される優先パケットと、この優先パケットよりも送信優先度が低い一般パケットとを時間軸上で多重して送信し、送信される優先パケットにおける優先データの平均送信データレートを、たとえば、専用ハードウェアを用いて平均入力レート以上の速度で送信するように制御する。ビデオ信号等のリアルタイム性を必要とするデータのプロトコル処理をC P Uによるソフトウェア処理に頼らずハードウェア処理を行うため、ソフトウェア処理で発生する処理が間に合わないという不具合が発生しない。これにより、全ての優先データパケットが完全に送信され、リアルタイム性の保証された高品質映像の伝送が可能となる。

また、一般データは一時的にバッファ手段に蓄積され、優先データ伝送が優先して行なわれる中で間欠的に伝送される。ここで、一般データの伝送レートが1 M b p s 以下の場合は、安価なC P Uやマイコンなどのプロセッサを用いて一般データの伝送処理が可能である。

なお、ストリームとして入力される優先データは、ストリームの無効データ部が除去され、有効データのみを用いて、パケット化情報に基づいてパケットが生成される。ここで、通信プロトコルとしてU D P / I Pを使用すると、ヘッダとしては、アドレスとしてI Pアドレス、また、サブアドレスとしてU D P ポート

番号を使用することとなる。

更に、優先パケットと一般パケットの送信タイミング（送信割合）をソフトウェアではなくハードウェアで制御するので、クロック単位で完全に制御可能である。これにより全ての優先パケットが完全に送信され、リアルタイム性の保証された高品質の伝送が可能となる。また、シェイピングもクロック単位で正確に行われるため、初段のルータでのパケット廃棄の発生確率が非常に少ない高品質な通信が可能となる。イーサネット（R）フレーム（2層）のレイヤでIP（3層）、UDP（4層）のヘッダを同時に検査し、優先パケットと一般パケットを分離し、優先パケットの処理をハードウェアで行うので、受信フレームの取りこぼしが発生せず、リアルタイム性が保証された高品質の通信が可能となる。

また、本発明のある実施の形態によれば、優先データと一般データを送信するだけでなく、有効データから優先データフォーマット情報を得て、外部から入力されるパケット化情報とともにパケット化パラメータの決定に使用する。これにより、たとえば、優先データがDV系の場合はDIFブロックの80バイト単位、また、MP EG系の場合はTSパケットの188バイト単位で優先データのパケット化の自動化などを行なうことができ、送受信装置の構成を簡単にすることができる。

本発明のある実施の形態によれば、送信装置内の優先データパケット化手段において、優先データにエラー訂正符号を付加することにより、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データを復元することが可能になる。

本発明のある実施の形態によれば、送信装置内の優先データパケット化手段における伝送エラー保護機能が実現できる。具体的には、優先データを暗号化した後、エラー訂正符号を付加することにより、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データを復元することが可能になるとともに、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現す

る。これにより、伝送路としてインターネットなどの公衆網を使用した場合においても、リアルタイム伝送される優先データ（ＡＶデータ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるＡＶデータの販売、課金が可能となり、安全性の高いＢ－Ｂ、Ｂ－Ｃのコンテンツ販売流通が可能となる。

本発明のある実施の形態によれば、暗号化を行なう暗号鍵を切り替えるにより、リアルタイム伝送される優先データ（ＡＶデータ）の盗聴、漏洩をより困難にすることができる。エラー訂正マトリックスの位相を暗号鍵の切替位相とすることにより、暗号鍵の切替をスムーズに実行できる。インターネットなどの公衆網において、リアルタイムに伝送されるＡＶデータの暗号化パラメータが変化するため、コンテンツの盗聴、漏洩を強力に防止できる。

本発明のある実施の形態によれば、受信装置での信号処理を簡単にすることが可能となる。優先データのフォーマットやチャンネル番号とポート番号の組み合わせを決めるテーブルを送信装置と受信装置に設けることにより、受信装置でポート番号を検出するだけでフォーマットの検出ができるため、受信装置での信号処理を簡単にすることが可能となる。また、２系統のストリーム処理が可能な受信装置で２つのストリームを同時に受信している場合でもポート番号でフォーマットまたはチャンネルを識別することが可能となる。

また、本発明のある実施の形態によれば、一般パケットは従来通りＣＰＵを用いてソフトウェア処理を行うのでソフトウェアを追加するだけで、管理情報および制御情報などのデータを一般データとして伝送させることができる。これらのデータ量は優先データ量に比べて非常に少ないので、マイコンなど安価なマイクロプロセッサで実現可能となり低コストなシステムを実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価なＣＰＵや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できる。

請求の範囲

1. 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

5 暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

10 前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも1つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

15 受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

20 前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段と
を備える、パケット送受信装置。

25 2. 前記パケット化手段は、前記送信条件設定情報および前記認証・鍵交換手段に関連する認証・鍵交換関連情報の少なくとも1つを用いて、パケット付加情報を生成するパケット付加情報生成手段を含み、

前記パケット化手段は、前記暗号化送信データに前記パケット付加情報を付加することによって、前記送信パケットを生成し、

前記パケット受信手段は、前記送信パケットに含まれるパケット付加情報を抽出するパケット付加情報抽出手段を含む、請求の範囲第1項に記載のパケット送受信装置。

3. 前記送信パケットを用いて送信フレームを生成するフレーム化手段と、
受信フレームを受け取り、前記受信フレームから前記受信パケットを抽出するフレーム受信手段と

をさらに備える、請求の範囲第1項に記載のパケット送受信装置。

4. 前記パケット化手段にて生成された第1のパケットを一時的に蓄積する第1のキュー手段と、

前記パケット化手段にて生成された第2のパケットを一時的に蓄積する第2のキュー手段と、

前記送信条件設定情報に基づいて、前記第1のキュー手段に蓄積された前記第1のパケットおよび前記第2のキュー手段に蓄積された前記第2のパケットのいずれを送信するかを制御する送信キュー制御手段と、

前記第1のキュー手段から出力された第1のパケットおよび第2のキュー手段から出力された第2のパケットをフレーム化することによって送信フレームを生成するフレーム化手段と、

受信フレームから前記受信パケットを抽出するフレーム受信手段と
をさらに備える、請求の範囲第1項に記載のパケット送受信装置。

5. 前記送信キュー制御手段は、前記第1のパケットまたは前記第2のパケットの送信経路に関する情報と、前記第1のパケットまたは前記第2のパケットを

送信するのに必要な帯域幅に関する情報と、前記送信パケットの送信から到着までの遅延に関する情報と、前記第1のパケットまたは前記第2のパケットの優先度に関する情報とのうち少なくとも1つの情報を用いて、前記第1のキュー手段に蓄積された前記第1のパケットおよび前記第2のキュー手段に蓄積された前記第2のパケットのいずれを送信するかを制御する、請求の範囲第4項に記載のパケット送受信装置。

6. 前記送信キュー制御手段は、IETF rfc2205、rfc2208、rfc2209で記載されたRSVP方式、IETF rfc2210、rfc2211、2212、rfc2215で記載されたIntserv方式、IETF rfc2474、rfc2475、rfc2597、rfc2598で記載されたDiffServ方式のいずれか1つの制御方式を使用する、請求の範囲第5項に記載のパケット送受信装置。

7. 前記送信キュー制御手段は、前記第1のキュー手段に蓄積された前記第1のパケットおよび前記第2のキュー手段に蓄積された前記第2のパケットのうちのいずれかを選択して、選択したパケットを優先的に出力するように前記第1のキュー手段および前記第2のキュー手段を制御する、請求の範囲第4項に記載のパケット送受信装置。

8. 前記送信キュー制御手段は、前記第2のキュー手段に蓄積された前記第1のパケットの量が所定の量を超えない場合には、前記第1のキュー手段に蓄積された前記第1のパケットを優先して出力し、前記第2のキュー手段に蓄積された前記第2のパケットの量が所定の量を超える場合には、前記第2のキュー手段に蓄積された前記第2のパケットを優先的に出力するように前記第1のキュー手段および前記第2のキュー手段を制御する、請求の範囲第4項に記載のパケット送

受信装置。

9. 前記送信キュー制御手段は、前記第1のキュー手段から送信される前記第1の
1の packets と前記第2のキュー手段から送信される前記第2の packets との間
5 隔を平均化するように前記第1のキュー手段および前記第2のキュー手段を制御
する、請求の範囲第4項に記載の packets 送受信装置。

10. 前記送信条件設定管理手段および前記受信条件設定管理手段は、前記送
信フレームの送信から到着するまでの間において前記送信 packets の送信先から
10 受信先までの経路における最大伝送 packets サイズの検出を行ない、前記最大伝
送 packets サイズ情報を用いて、前記送信条件設定情報および前記受信条件設定
情報を生成する、請求の範囲第1項に記載の packets 送受信装置。

11. 前記フレーム化手段は、前記 packets 化手段にて生成された前記送信パ
15 ckets に、IEEE 802.3規格のフレームヘッダを付加する、請求の範囲
第3項に記載の packets 送受信装置。

12. 前記フレーム化手段は、前記 packets 化手段にて生成された前記送信パ
ckets に、IEEE 802.1Q規格のフレームヘッダを付加する、請求の範
20 囲第3項に記載の packets 送受信装置。

13. 前記 packets 化手段は、前記暗号化送信データを所定の大きさに変換し、
IETFでIPv4またはIPv6として規定されているIP (Internet
t Protocol) ヘッダを付加する、請求の範囲第1項に記載の packets
25 送受信装置。

14. 前記パケット化手段は、IPv4ヘッダのサービスタイプフィールド、または、サービスタイプフィールド内のTOS (Type of Service) フィールドに優先パケットであることを示す情報を付加する、請求の範囲第1項に記載のパケット送受信装置。

5

15. 前記パケット化手段は、IPv6ヘッダのプライオリティフィールドに優先パケットであることを示す情報を付加する、請求の範囲第1項に記載のパケット送受信装置。

10 16. 前記パケット化手段は、第1のパケット化手段と、第2のパケット化手段とを含み、

前記第1のパケット化手段は、前記送信条件設定情報および前記認証・鍵交換関連情報の少なくとも一つの情報を用いて前記第1のパケットを生成し、

15 前記第2のパケット化手段は、前記送信条件設定情報と、前記認証・鍵交換関連情報と、前記暗号化送信データとの少なくとも一つの情報を用いて前記第2のパケットを生成する、請求の範囲第4項に記載のパケット送受信装置。

17. 前記パケット化手段は、前記暗号化送信データを所定の大きさに変換し、IETFでIPv4またはIPv6として規定されているIPヘッダを付加し、

20 前記第1のパケット化手段はソフトウェアによって構成され、前記第2のパケット化手段はハードウェアによって構成される、請求の範囲第16項に記載のパケット送受信装置。

25 18. 前記送信データを優先データと一般データとに分離するデータ分離手段をさらに備え、

前記暗号化手段は、前記優先データを暗号化し、

前記第1の packets 化手段は、前記一般データを用いて第1の packets を生成する、請求の範囲第16項に記載の packets 送受信装置。

19. 前記第1の packets 化手段は、IETF 文書で規定されているデータ処理
5 理プロトコルである RTP, RTSP, HTTP, TCP, UDP, IP のうちの少なくとも1つのヘッダを付加する、請求の範囲第18項に記載の packets 送受信装置。

20. 前記第2の packets 化手段は、データにシーケンス番号を付加するか、
10 または、IETF 文書で規定されているデータ処理プロトコルである RTP, UDP, HTTP, TCP, IP のうちの少なくとも1つのヘッダを付加する、請求の範囲第18項に記載の packets 送受信装置。

21. 前記優先データは、SMPTE 259M 規格で規定された非圧縮 SD
15 方式信号、または、SMPTE 292M 規格で規定された非圧縮 HD 形式、または、IEC 61883 規格で規定された IEEE 1394 による DV または MPEG-TS の伝送ストリーム形式、または、DVB 規格 A010 で規定された DVB-ASI による MPEG-TS 形式、MPEG-PS 形式、MPEG-ES 形式、MPEG-PES 形式の内の少なくとも一つのデータストリーム形式
20 である、請求の範囲第18項に記載の packets 送受信装置。

22. 前記第2の packets 化手段は、エラー訂正符号付加手段を含む、請求の範囲第16項に記載の packets 送受信装置。

23. 前記エラー訂正符号付加手段で用いられるエラー訂正符号の方式は、リードソロモン方式、あるいはパリティ方式である、請求の範囲第22項に記載の

パケット送受信装置。

24. 前記暗号化鍵を示す情報は、前記フレーム化手段において前記暗号化鍵で暗号化された送信パケットを出力するより前に、前記暗号化鍵の復号情報を前記フレーム化手段から出力する、請求の範囲第16項に記載のパケット送受信装置。

25. 前記暗号化鍵を示す情報は、前記暗号化鍵を用いて生成された前記暗号化送信データを含む送信パケットが送信されるときよりも、前記送信フレームの送信から前記送信フレームに対応する受信フレームの受信までの時間より前に送信される、請求の範囲第24項に記載のパケット送受信装置。

26. 前記認証・鍵交換手段は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可する、請求の範囲第1項に記載のパケット送受信装置。

27. 前記送受信管理情報は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報との少なくとも一方を含んでいる、請求の範囲第26項に記載のパケット送受信装置。

28. 前記位置情報は、地域コード、住所、郵便番号、または、経度・緯度により範囲が指定された情報である、請求の範囲第27項に記載のパケット送受信装置。

29. 前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケッ

トの到着先または前記受信パケットの送信元との間で、前記パケット送受信装置から前記送信パケットの到着先または前記受信パケットの受信元までの片道または往復の伝播時間があらかじめ決められた制限時間より短い時間である場合に、認証を許可する、請求の範囲第 26 項に記載のパケット送受信装置。

5

30. 前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間の送受信区間において無線伝送区間が存在する場合、前記無線伝送区間ではデータをスクランブルして伝送するモードであることを確認した場合に、認証を許可する、請求の範囲第 26 項に記載のパケット送受信装置。

10

31. 前記認証・鍵交換手段は、

前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間で認証を行った場合に、前記送信パケットの到着先または前記受信パケットの送信元に関する情報を一時的に記憶する記憶手段と、

15

前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元とが前記あらかじめ決められた条件に合致しないために前記認証が成立しない場合に、前記記憶手段にて記憶された情報と、前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報とを照合し、前記パケット送受信装置と前記送信パケットの到着先または前記受信パケットの送信元との間で認証を行う、照合手段とを含む、請求の範囲第 26 項に記載のパケット送受信装置。

20

32. 前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報は、証明書、MAC アドレスおよび生体情報の少なくとも 1 つを含む、請求の範囲第 31 項に記載のパケット送受信装置。

25

3 3. 前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期間で暗号化鍵または復号鍵を更新する、請求の範囲第 1 項に記載の packets 送受信装置。

5

3 4. 前記認証・鍵交換手段が前記復号鍵を更新するタイミングを示すタイミング情報が、前記送信 packets に付加される、請求の範囲第 3 3 項に記載の packets 送受信装置。

10

3 5. 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信 packets の TCP ポート番号、または UDP ポート番号を変化させることによって通知される、請求の範囲第 3 3 項に記載の packets 送受信装置。

15

3 6. 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信 packets が HTTP を使用している場合、HTTP リクエスト毎に更新される、請求の範囲第 3 3 項に記載の packets 送受信装置。

20

3 7. 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信 packets が HTTP を使用している場合、一定のデータ量毎に変化される、請求の範囲第 3 3 項に記載の packets 送受信装置。

25

3 8. 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信 packets が RTP を使用している場合、予め決められた期間内に更新される、請求の範囲第 3 3 項に記載の packets 送受信装置。

3 9. 前記認証・鍵交換手段における D T C P 方式のコピー制御情報は、前記

送信パケットに暗号化モード情報を付加することによって伝送される、請求の範囲第 3 3 項に記載のパケット送受信装置。

40. 前記優先データのデータレートが所定の値より小さくならないように、
5 前記送信キュー制御手段は前記第 1 のキュー手段および前記第 2 のキュー手段を制御する、請求の範囲第 1 8 項に記載のパケット送受信装置。

41. 前記送信キュー制御手段は、前記優先データが前記第 2 のキュー手段に蓄積される時間があらかじめ決めた値より常に小さくなるように、前記送信キュー
10 制御手段は前記第 1 のキュー手段および前記第 2 のキュー手段を制御する、請求の範囲第 4 0 項に記載のパケット送受信装置。

42. 前記第 2 のパケット化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、前記第 2 のパケットのパ
15 ケットヘッダを生成するパケットヘッダ生成手段と、前記パケットヘッダと前記バッファから出力されるペイロードとを組み合わせるパケットを合成するパケット合成手段とを含み、

前記パケットヘッダ生成手段は前記第 2 のパケットのペイロード長を指定して、前記バッファ手段に蓄積されたデータを読み出して、前記パケット合成手段に入
20 力する、請求の範囲第 4 0 項に記載のパケット送受信装置。

43. 前記第 2 のパケット化手段は、前記優先データから抽出したデータを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、パケット化情報を用いてパケットヘッダを生成するパケットヘッダ生成手段
25 と、前記パケットヘッダとペイロードとを組み合わせるパケットを生成するパケット生成手段とを含み、

前記カウンタ手段は前記バッファ手段からペイロード長に相当するデータを読み出すための制御データを出力する、請求の範囲第40項に記載の packets 送受信装置。

5 44. 前記第2の packets 化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、 packets 化情報を用いて packets ヘッダを生成する packets ヘッダ生成手段と、前記データにエラー訂正を付加するエラー訂正付加手段と、前記 packets ヘッダと前記エラー訂正を付加したデータとを合成する packets 合成手段とを含み、

10 前記カウンタ手段は前記バッファ手段よりペイロード長に相当するデータを読み出すための制御データを出力する、請求の範囲第40項に記載の packets 送受信装置。

15 45. 前記優先データおよび前記一般データが処理されるレイヤよりも下位レイヤの受信フレームを処理するレイヤにおいて、前記受信フレームに含まれる受信 packets の通信プロトコルヘッダから前記優先データと前記一般データを選別して、前記優先データの処理と前記一般データの処理を独立に行う、請求の範囲第40項に記載の packets 送受信装置。

20 46. 前記第2の packets 化手段は、暗号鍵切替手段を含み、前記暗号鍵切替手段に入力される暗号鍵を指定されたタイミングで切り替えながら前記暗号化手段に入力し、前記暗号化手段における暗号化鍵を指定の間隔で切替る、請求の範囲第1項に記載の packets 送受信装置。

25 47. 前記暗号鍵切替に用いるタイミングとしては、前記 packets ヘッダ生成手段の出力である packets ヘッダ内の所定のシーケンス番号に同期して発生した

タイミングである、請求の範囲第46項に記載の packets 送受信装置。

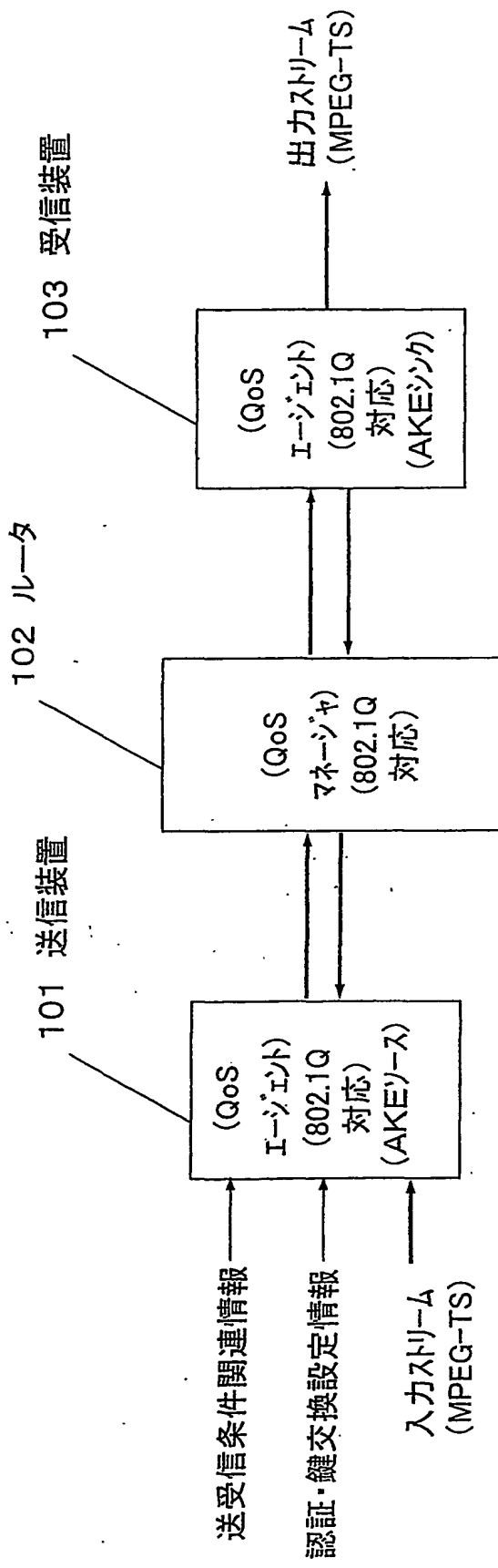
48. 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信 packets が HTTP を使用している場合、HTTP リクエスト毎に更新される、
5 請求の範囲第46項に記載の packets 送受信装置。

49. 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信 packets が HTTP を使用している場合、一定のデータ量毎に変化される、請求
10 の範囲第46項に記載の packets 送受信装置。

50. 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信 packets が RTP を使用している場合、予め決められた期間内に更新される、請求
15 の範囲第46項に記載の packets 送受信装置。

51. 前記暗号鍵切替に用いるタイミングとしては、エラー訂正マトリックス
の終点または始点に同期して発生したタイミングである、請求の範囲第46項に
記載の packets 送受信装置。

図1



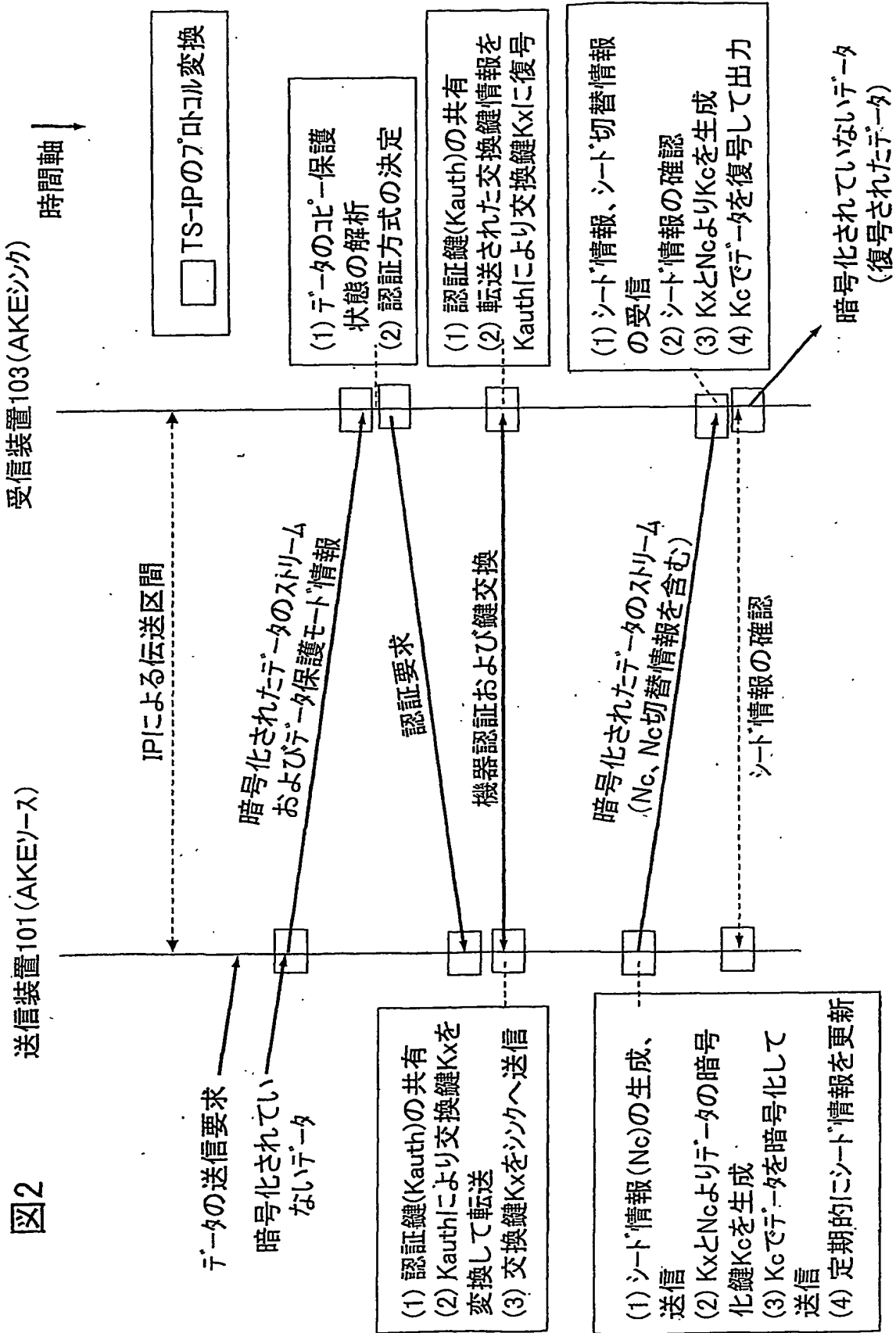


図3

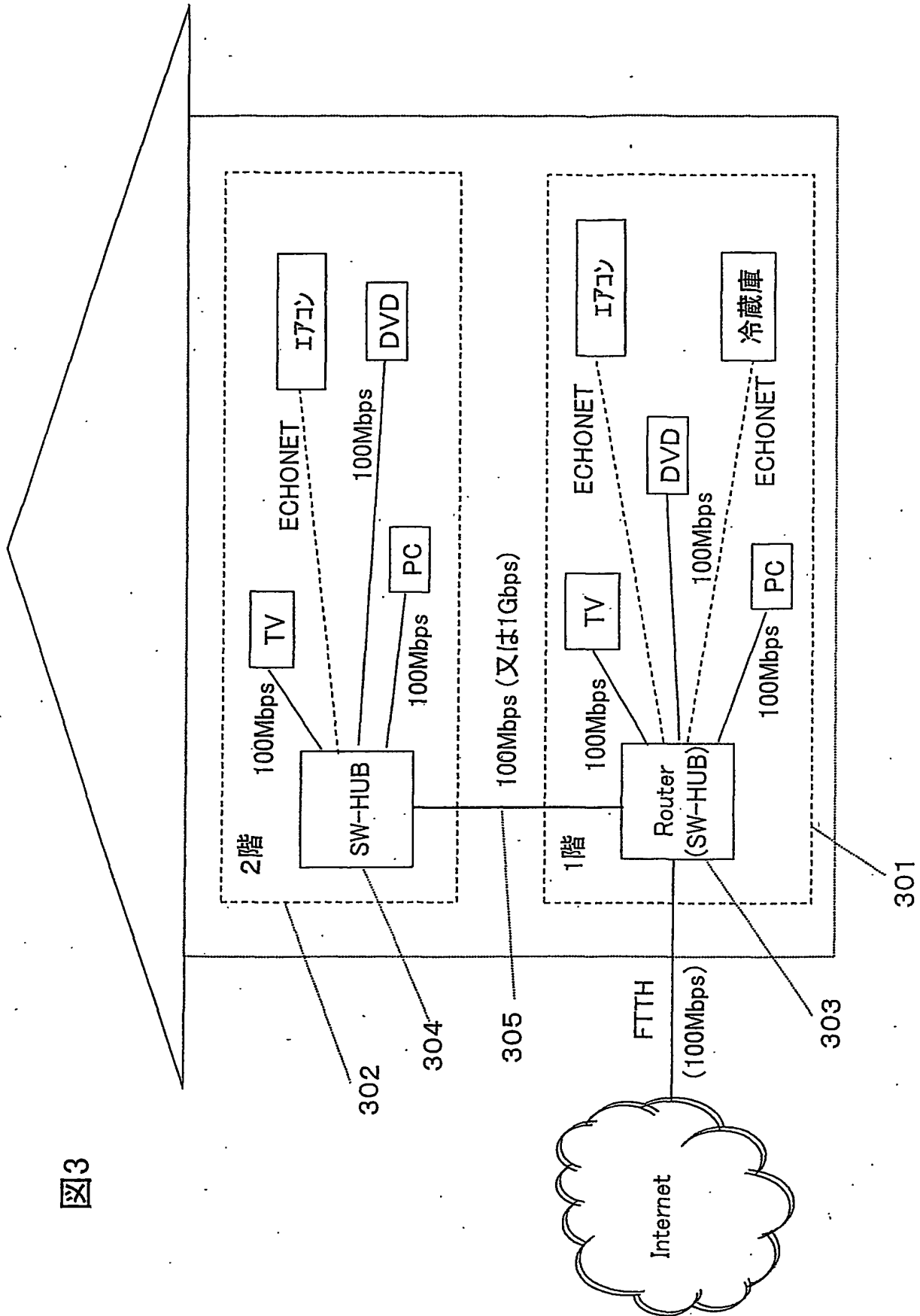


図4

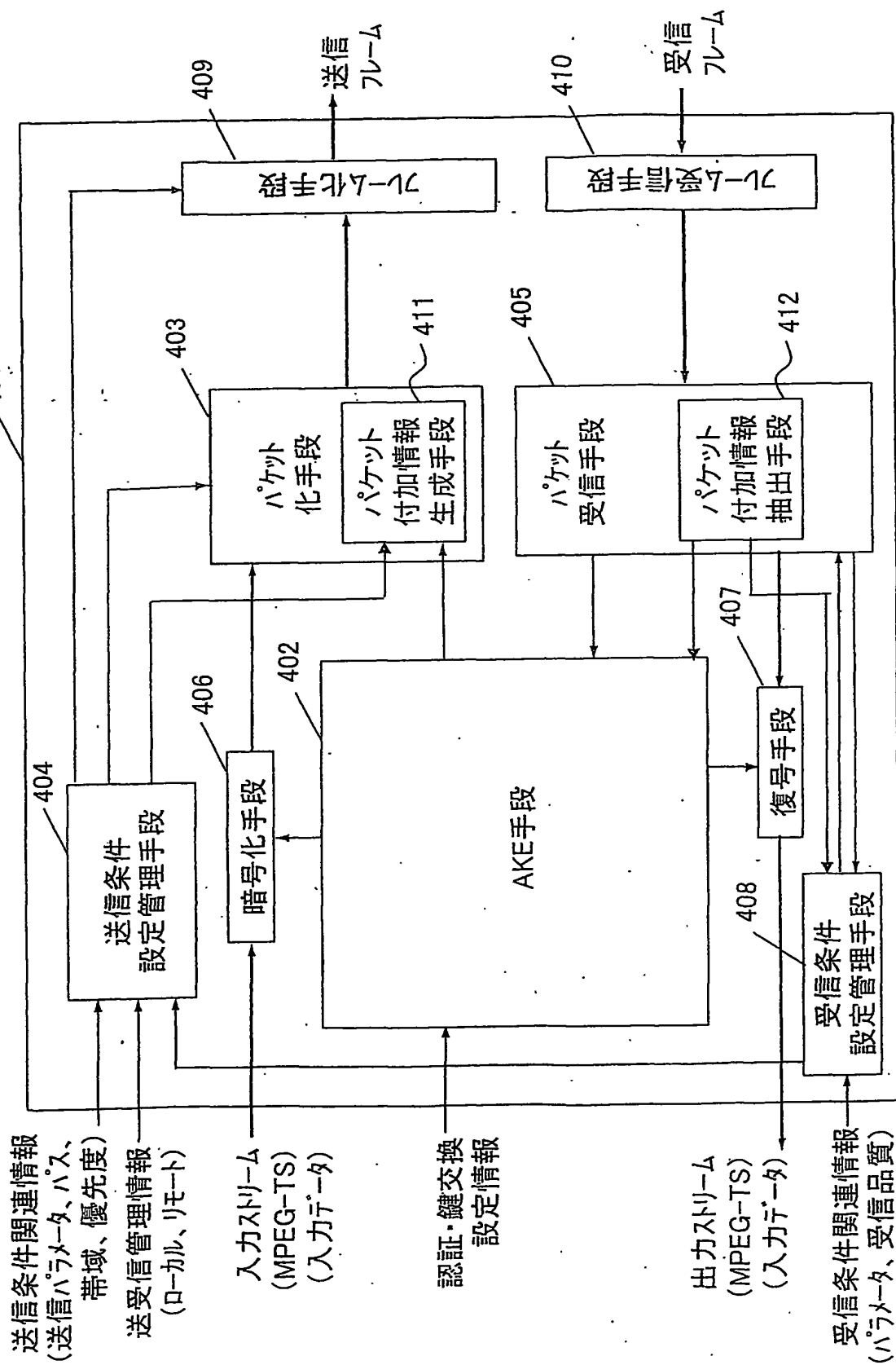


図5

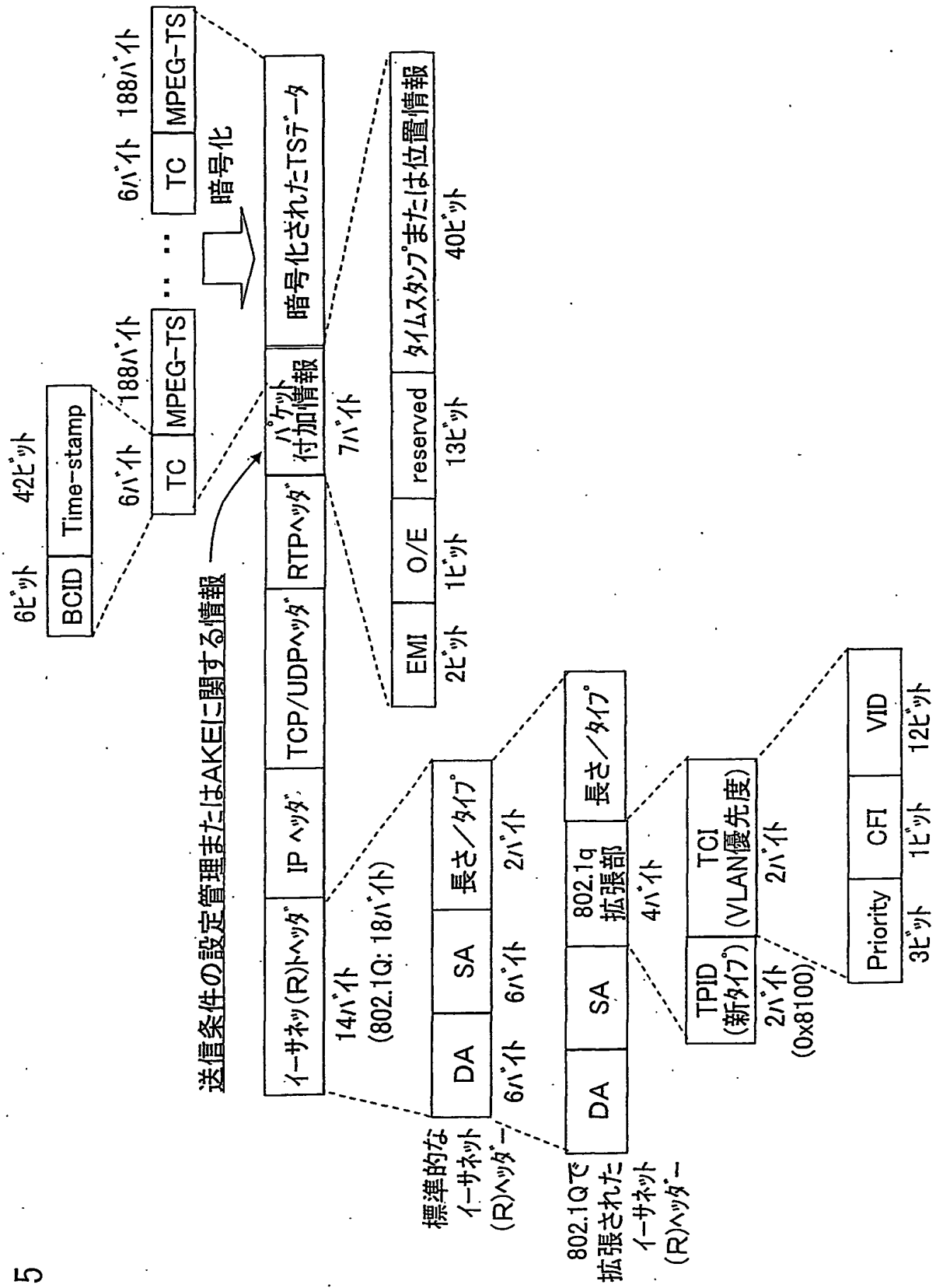
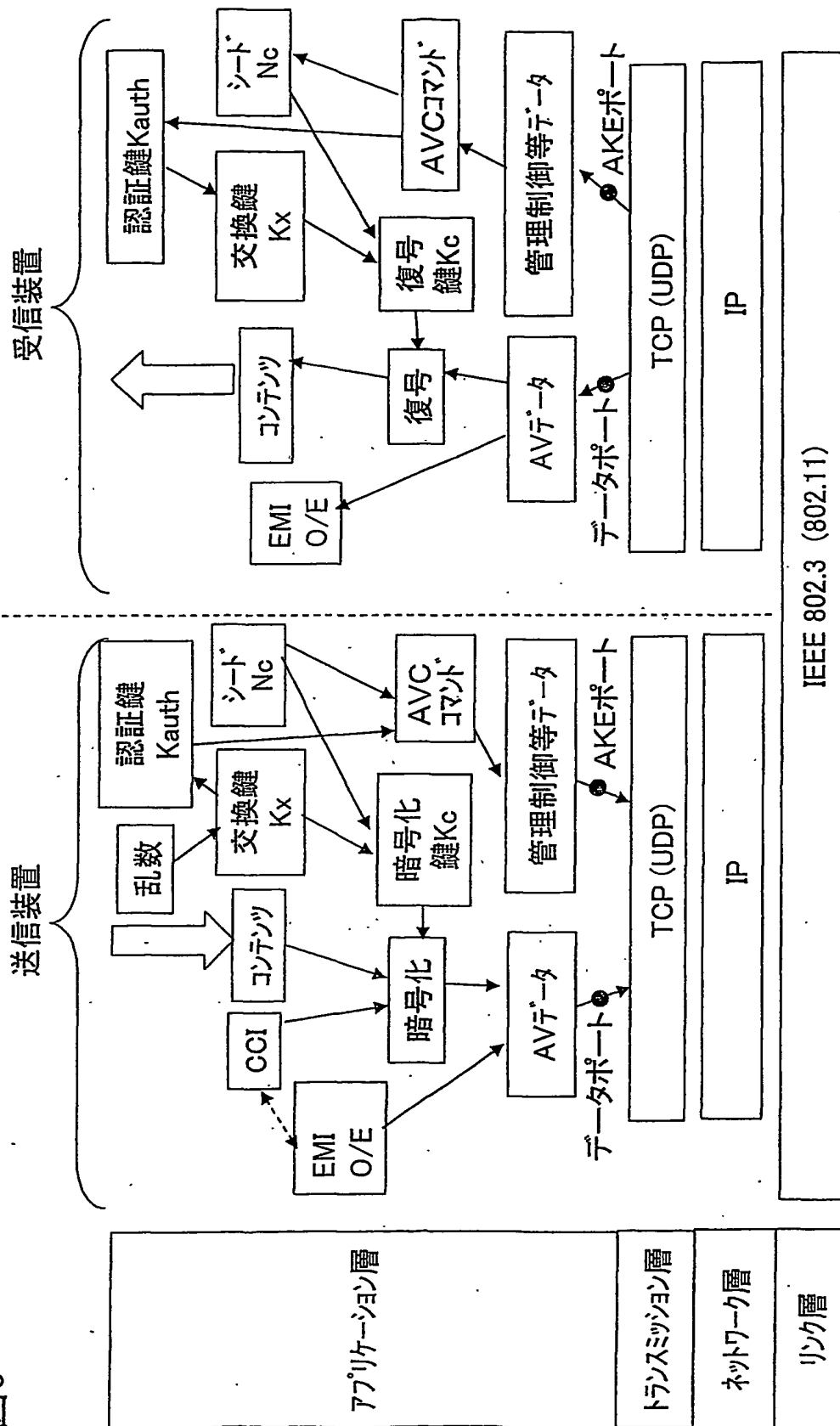
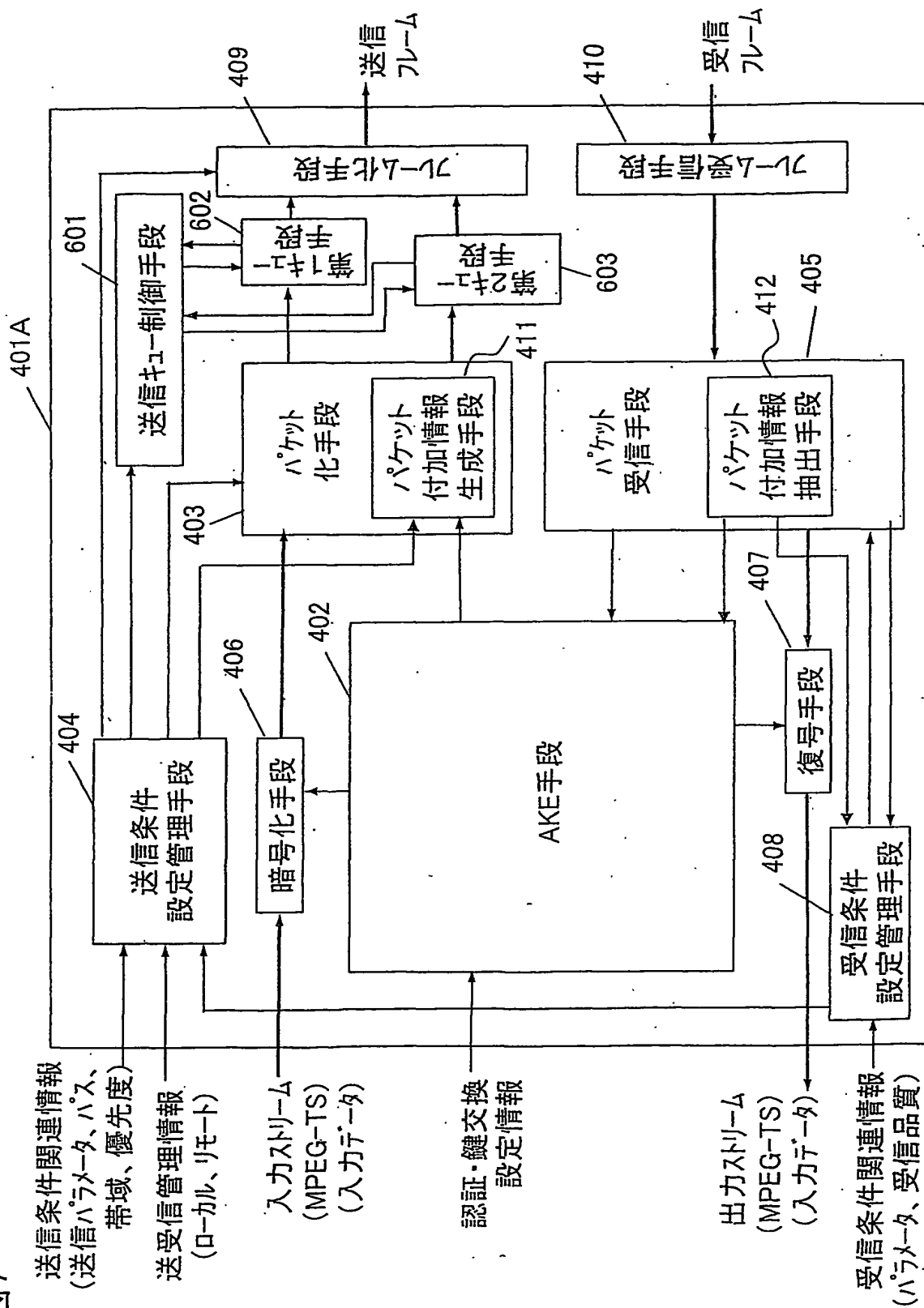


図6

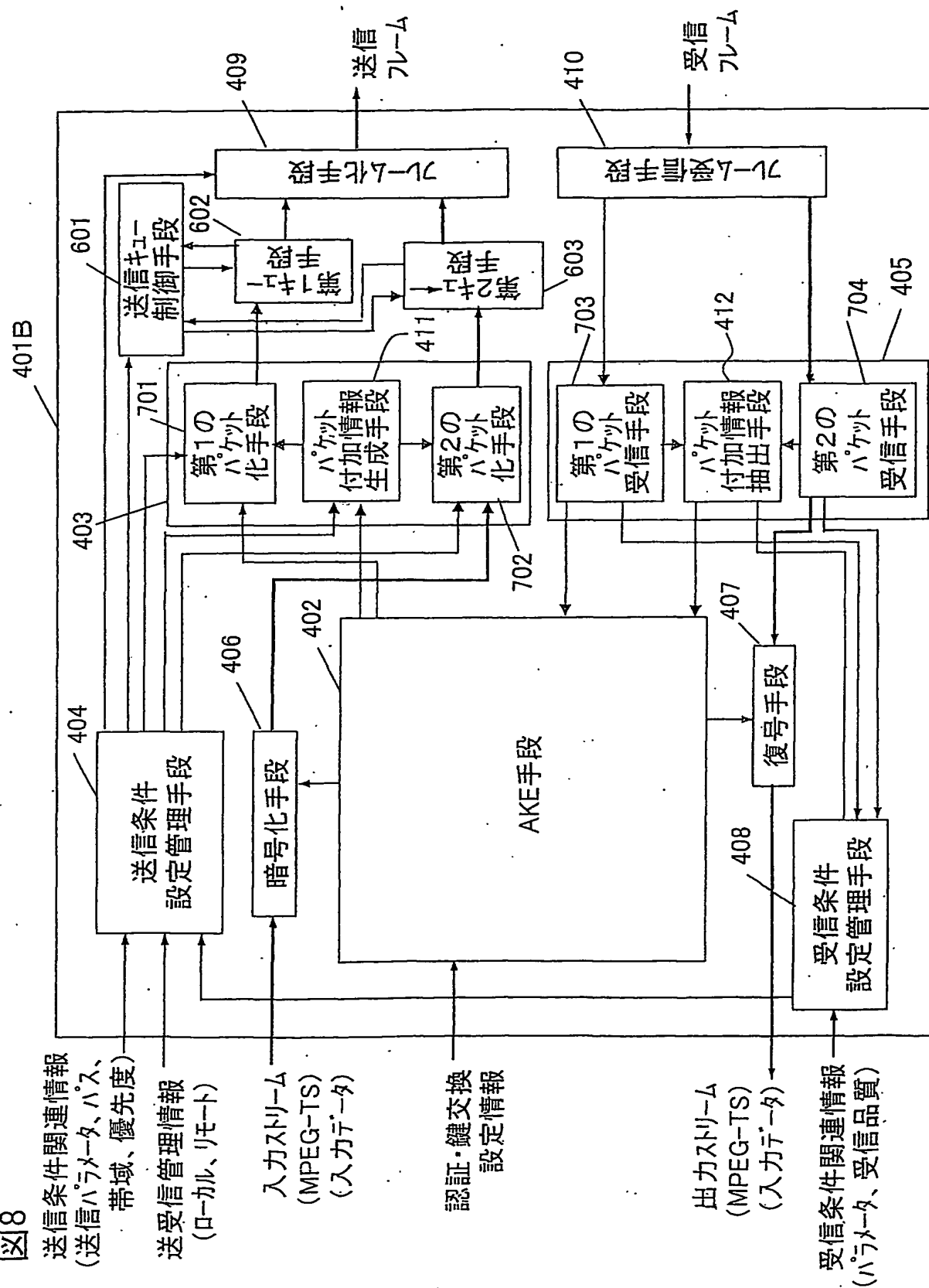


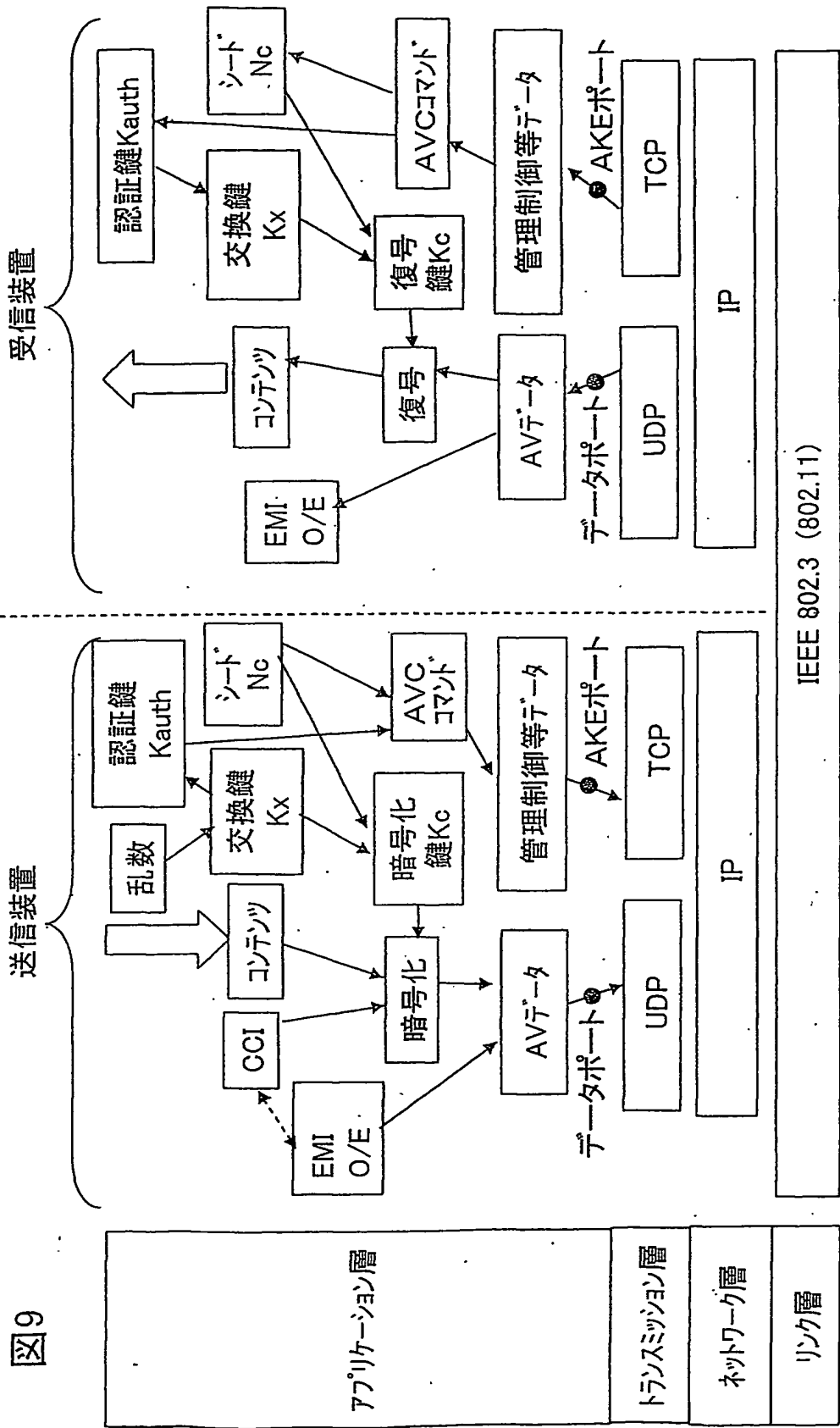
(OSIモデルによる説明)

図7



8
X





(OSIモデルによる説明)

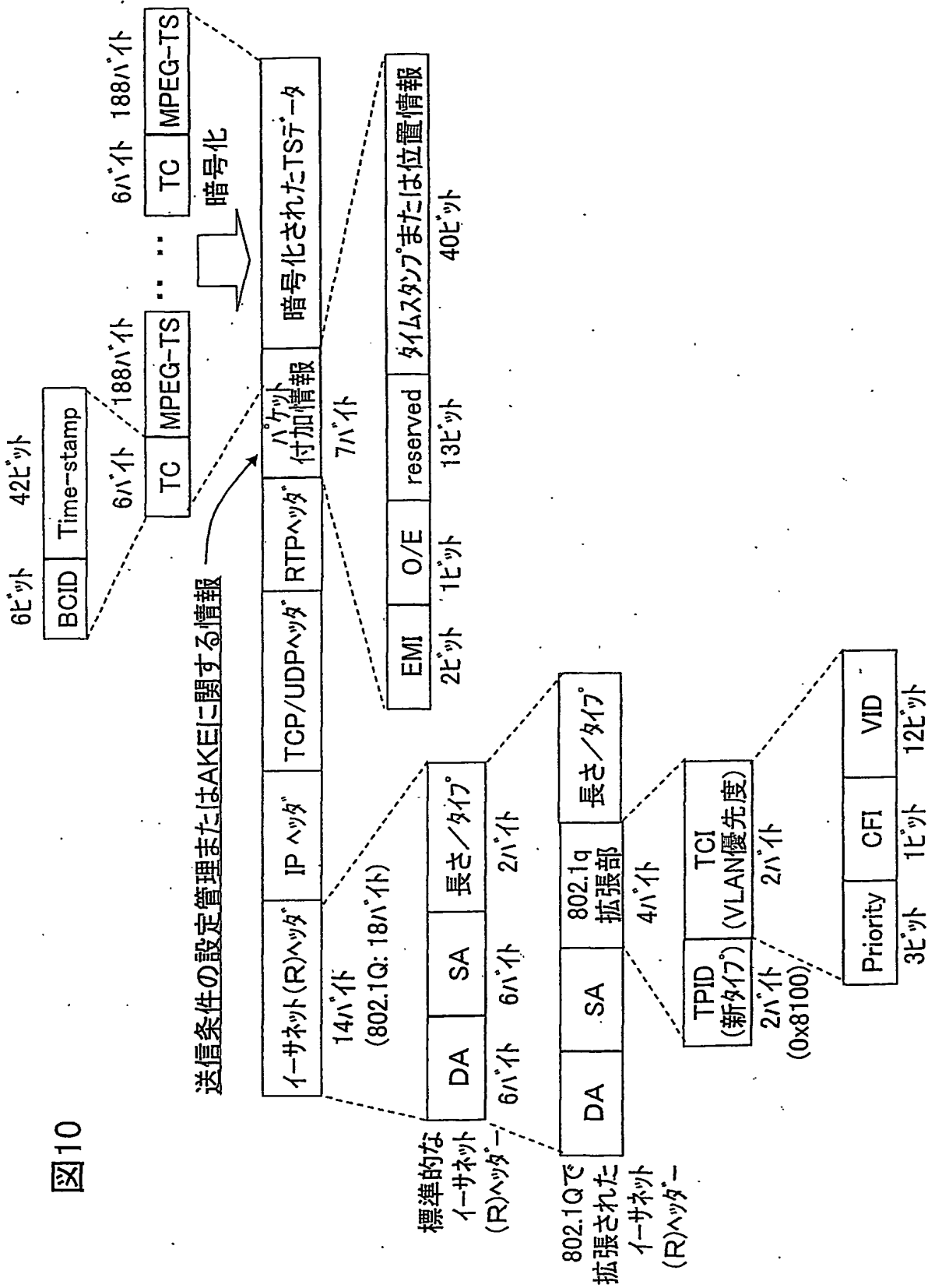
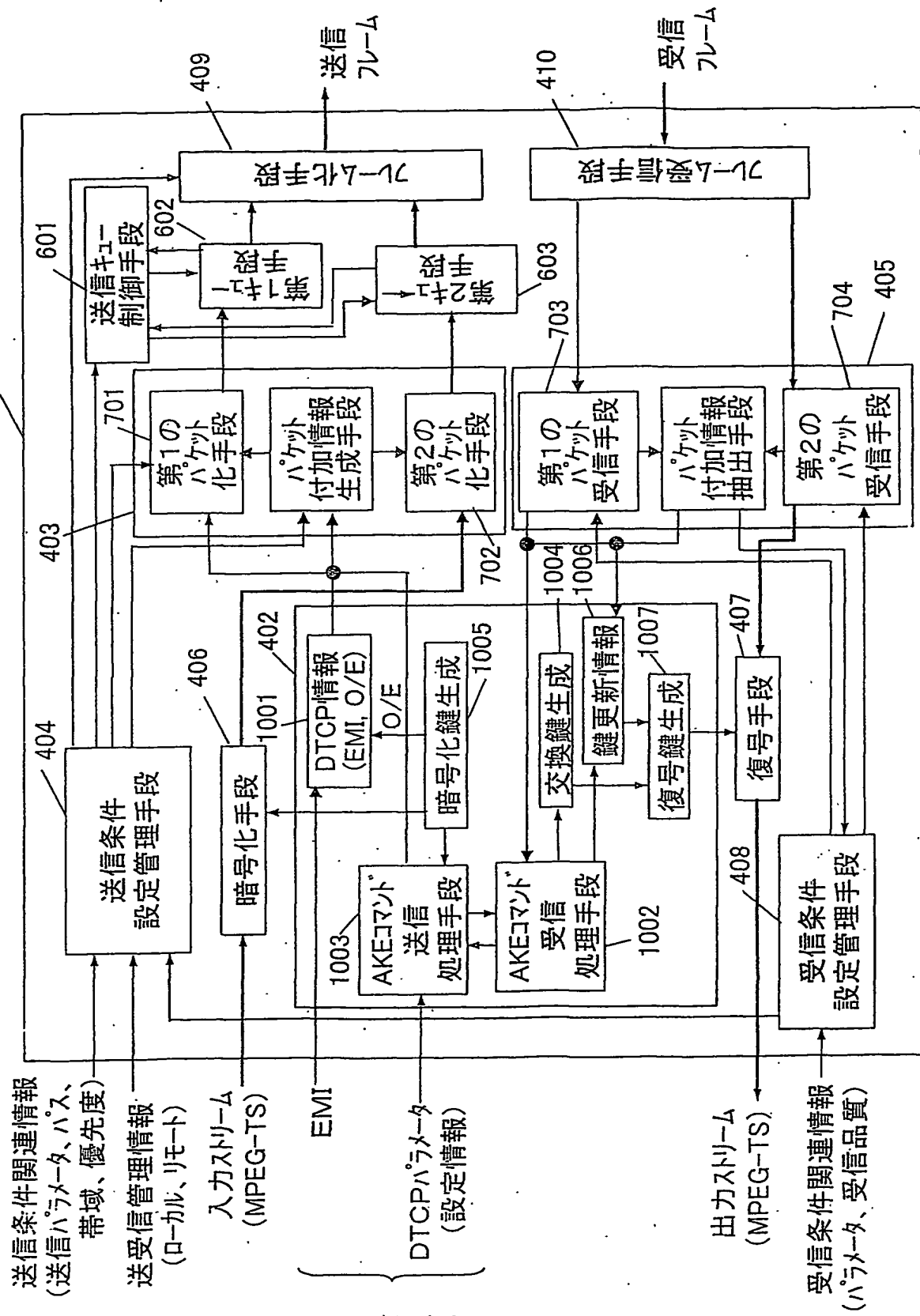
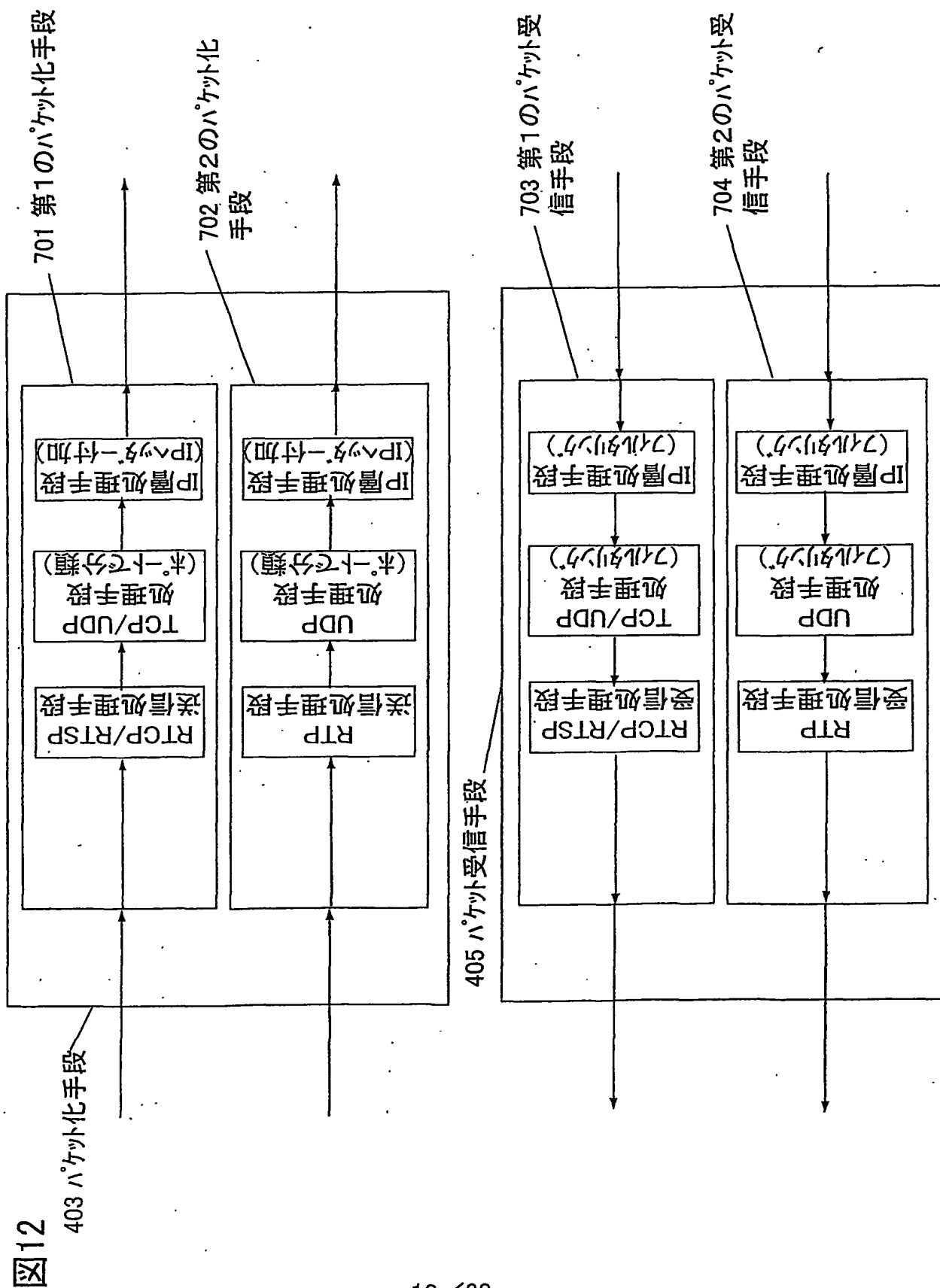
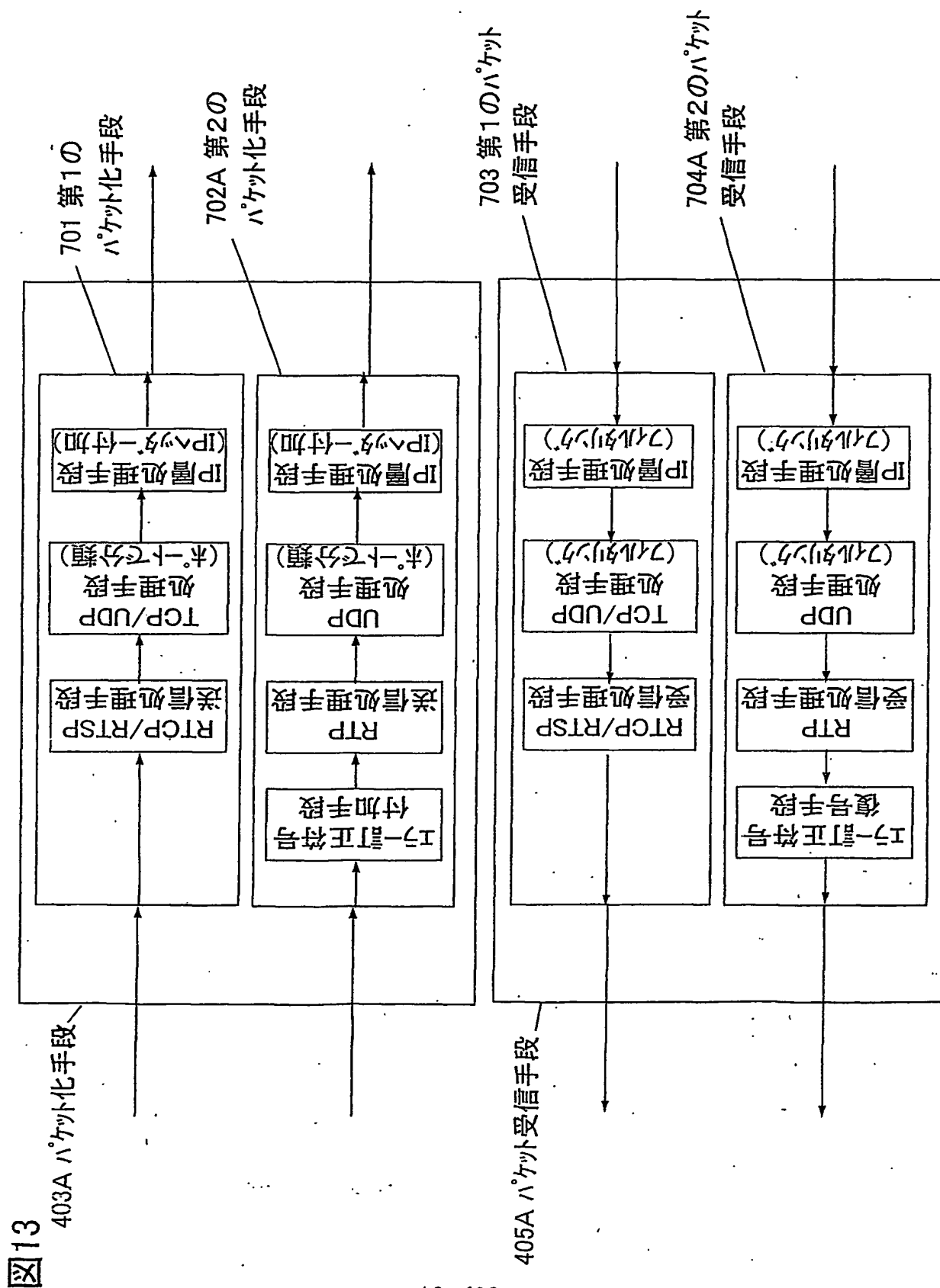
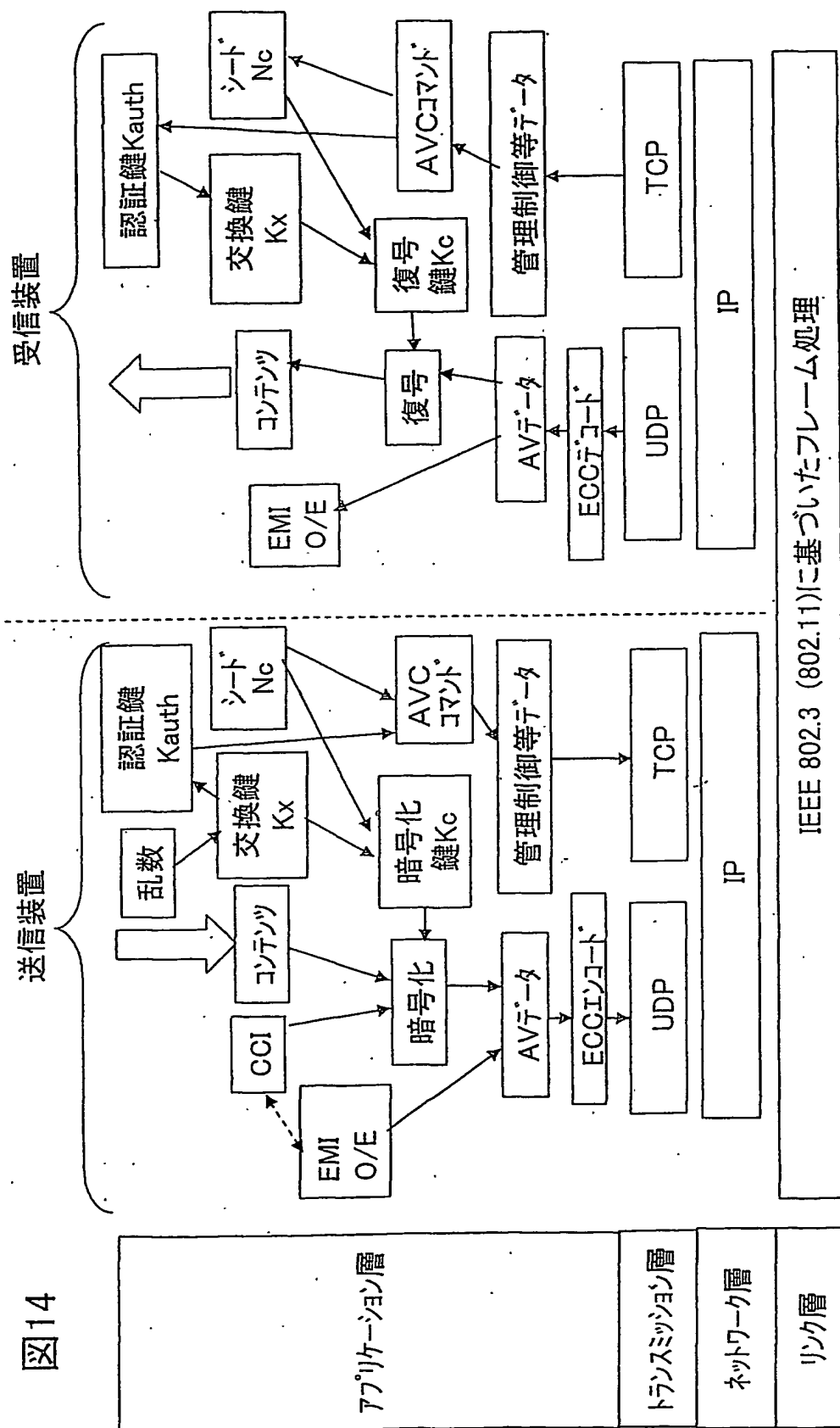


図11









(OSIモデルによる説明)

図15

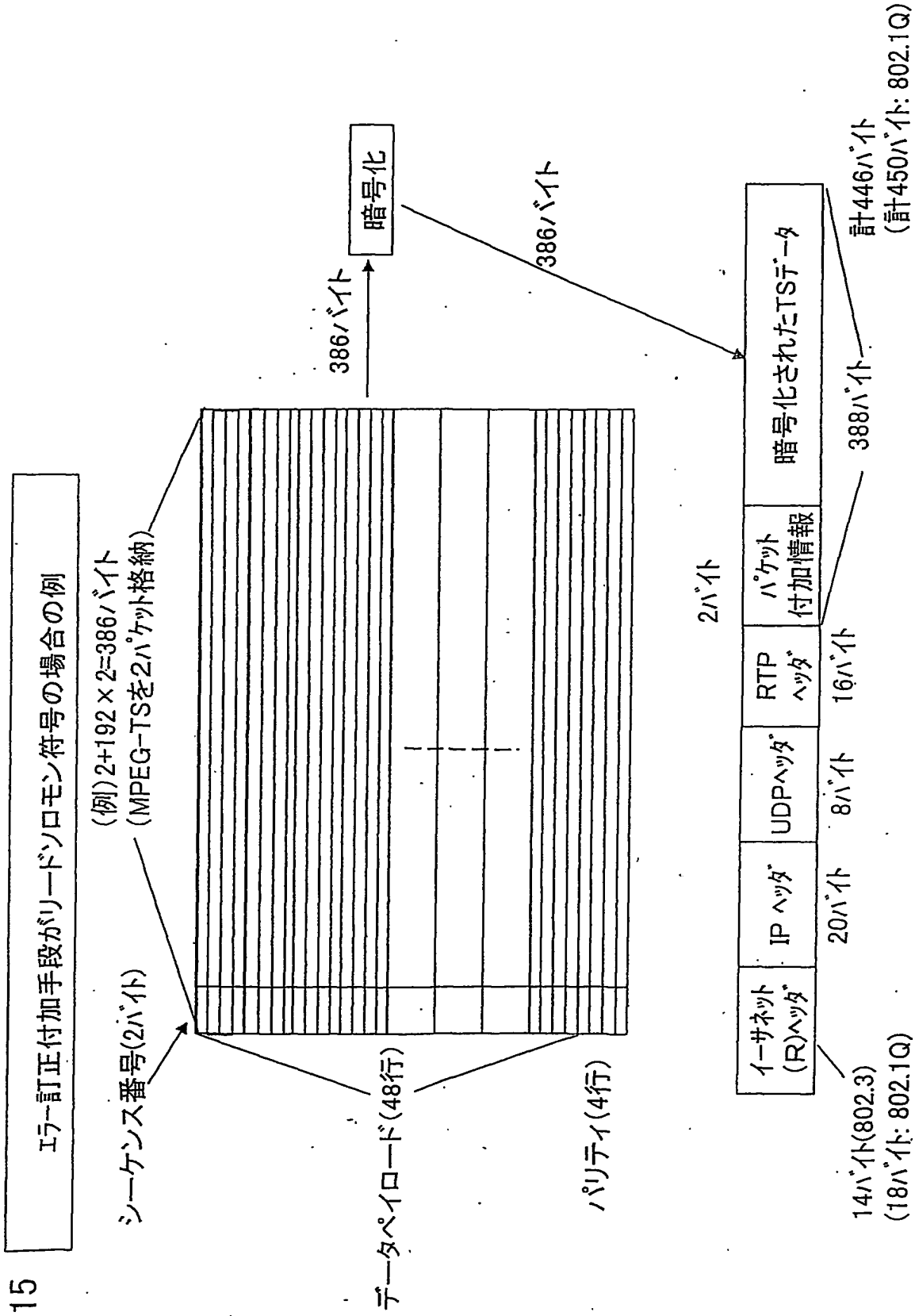
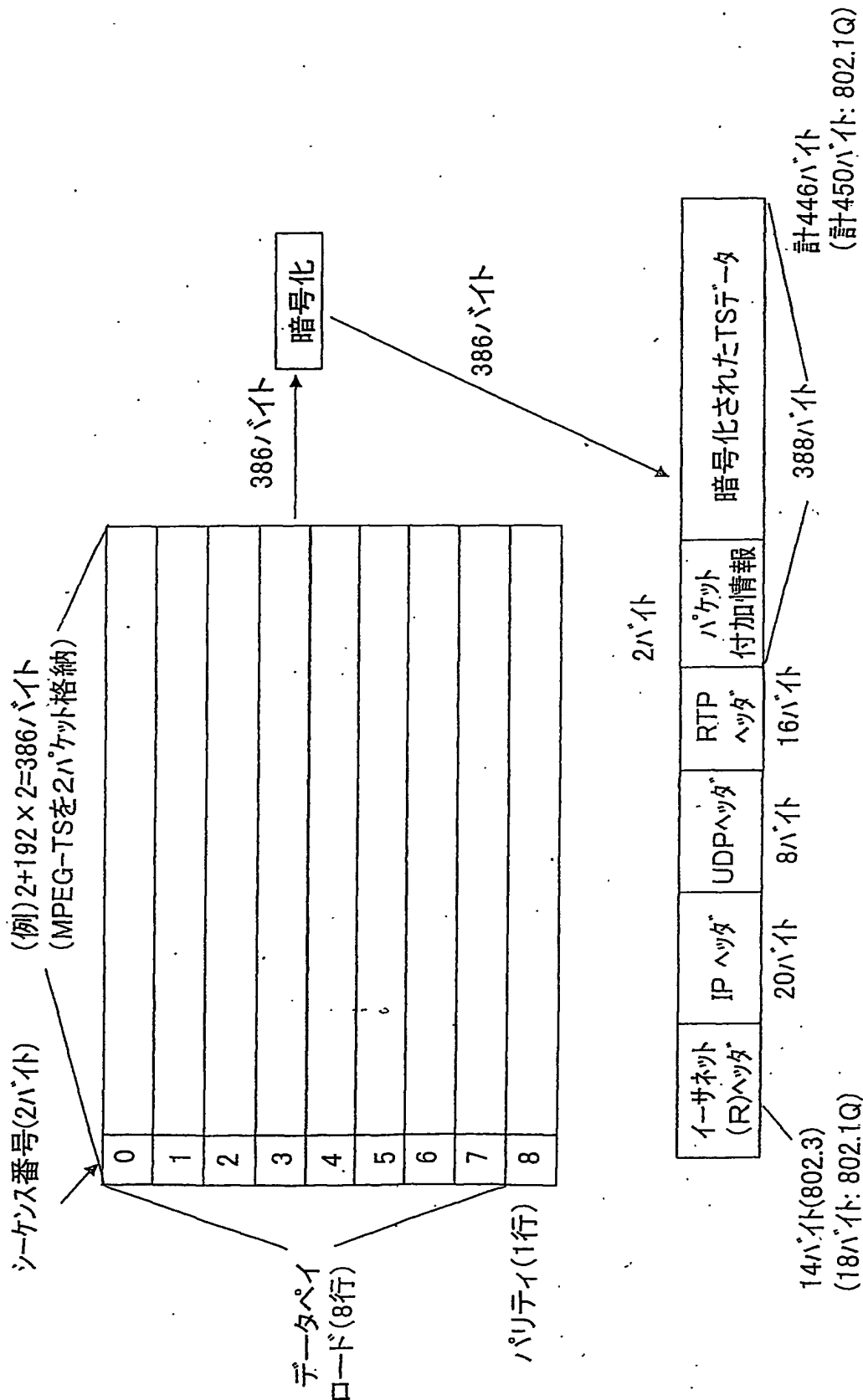


図16

エラー訂正付加手段がパリティの場合



17
[X]

送信条件関連情報
(送信パラメータ、パス、
帯域、優先度)

送受信管理情報
(ローカル、リモート)

入力ストリーム
(MPEG-TS)

DTCPパターナタ
(設定情報)

出力ストリーム
(MPEG-TS)

受信条件関連情報
(パラメータ、受信品質)

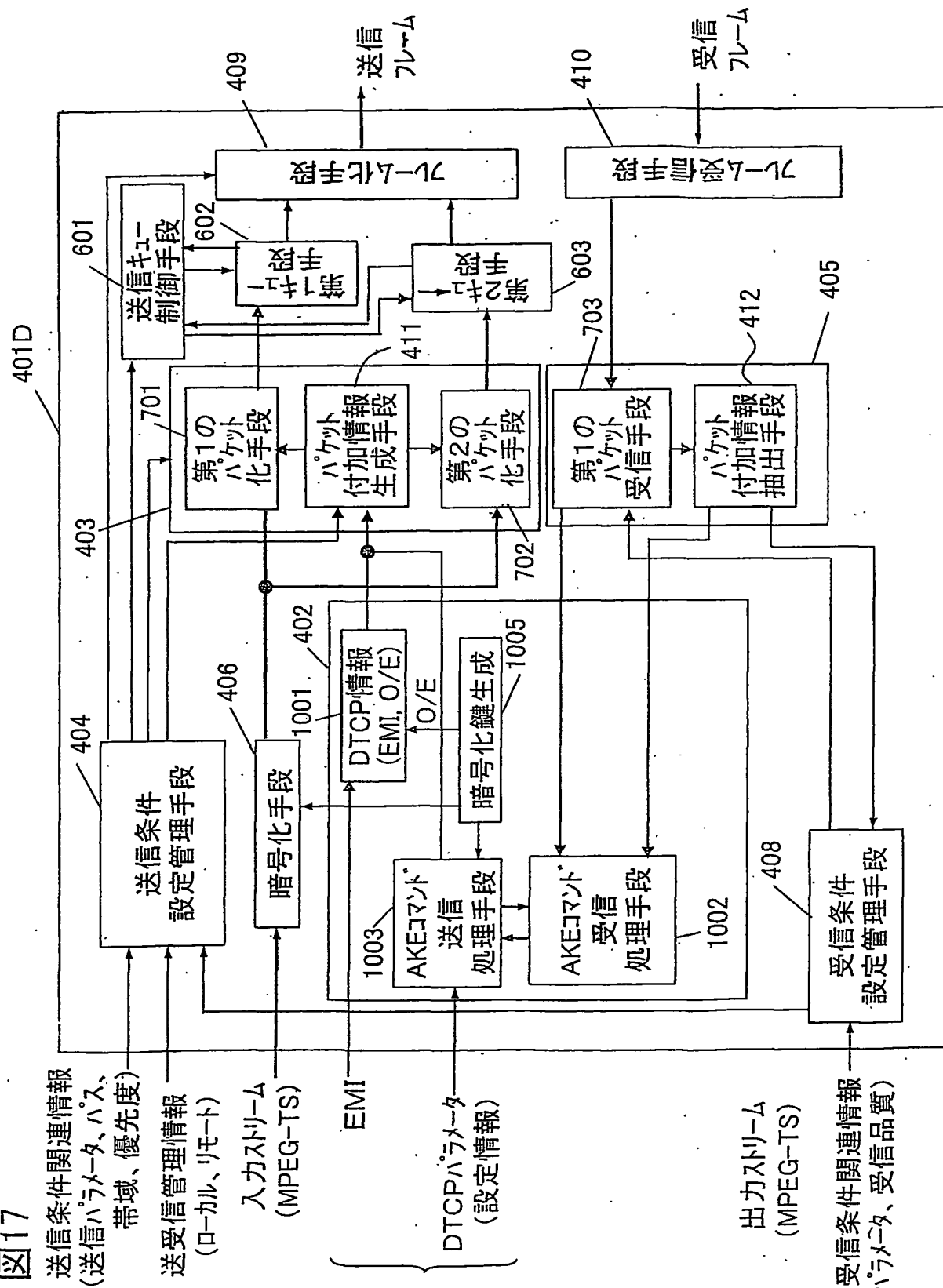


図18

送信条件関連情報
(送信パラメータ、パス、
帯域、優先度)
送受信管理情報
(ローカル、リモート)

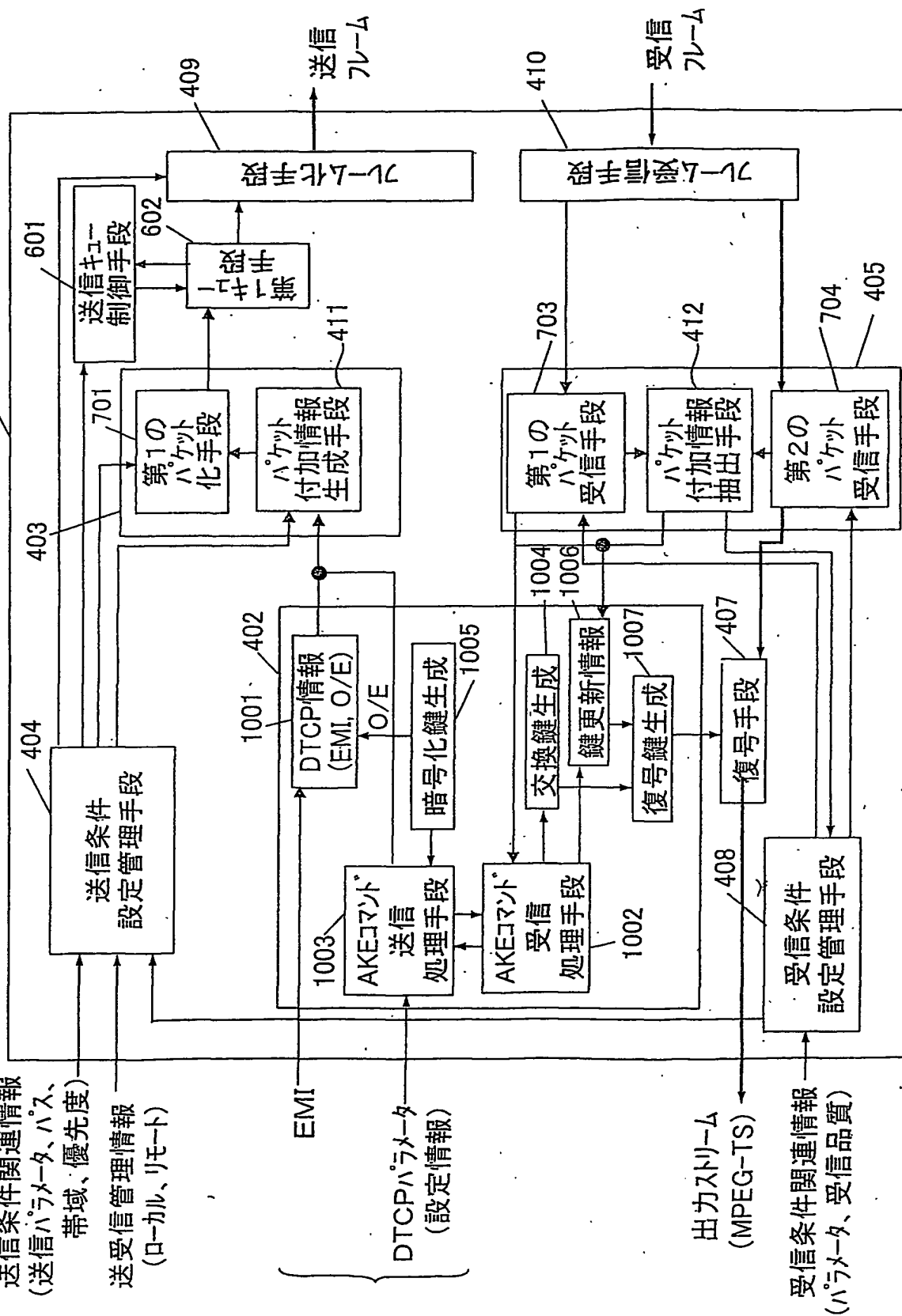


図19

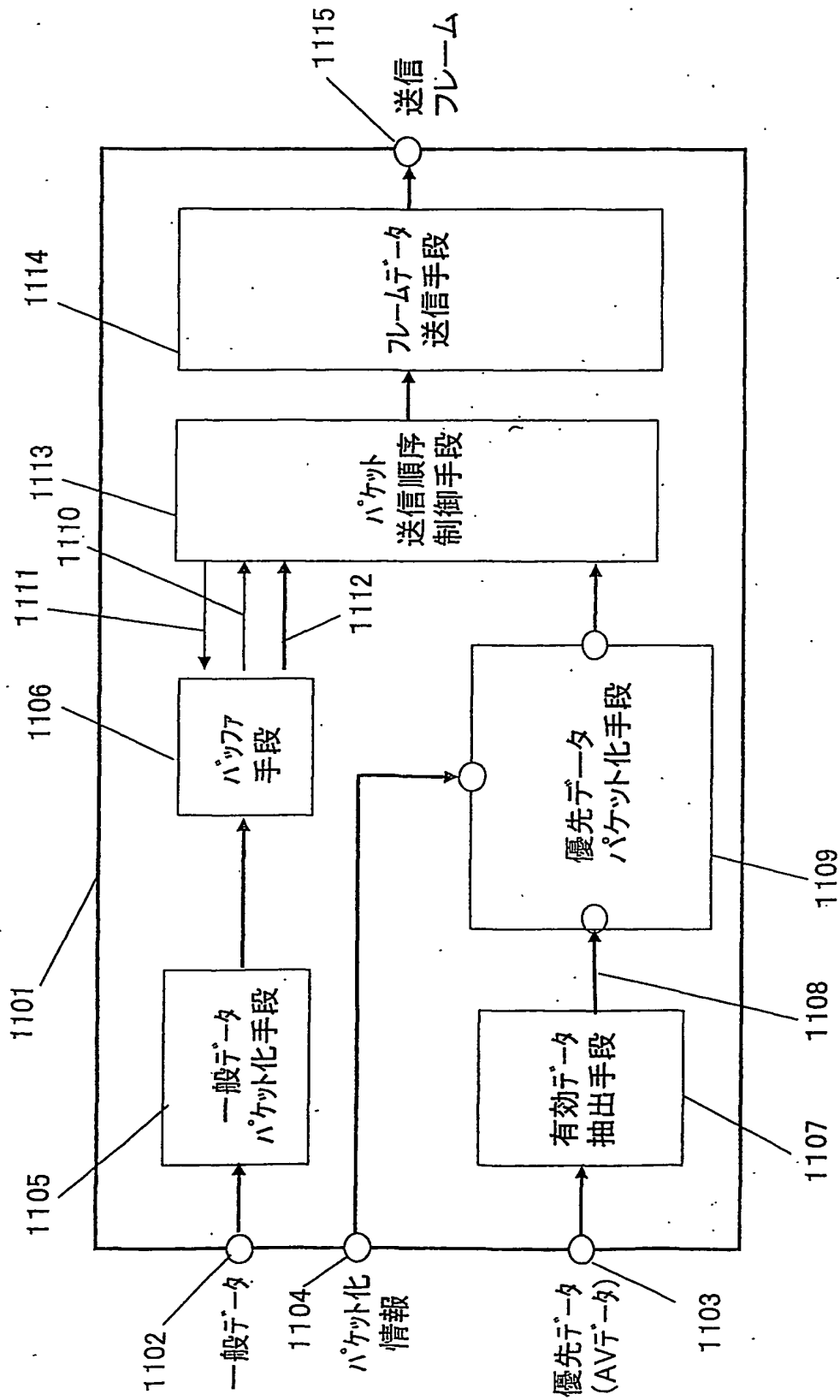
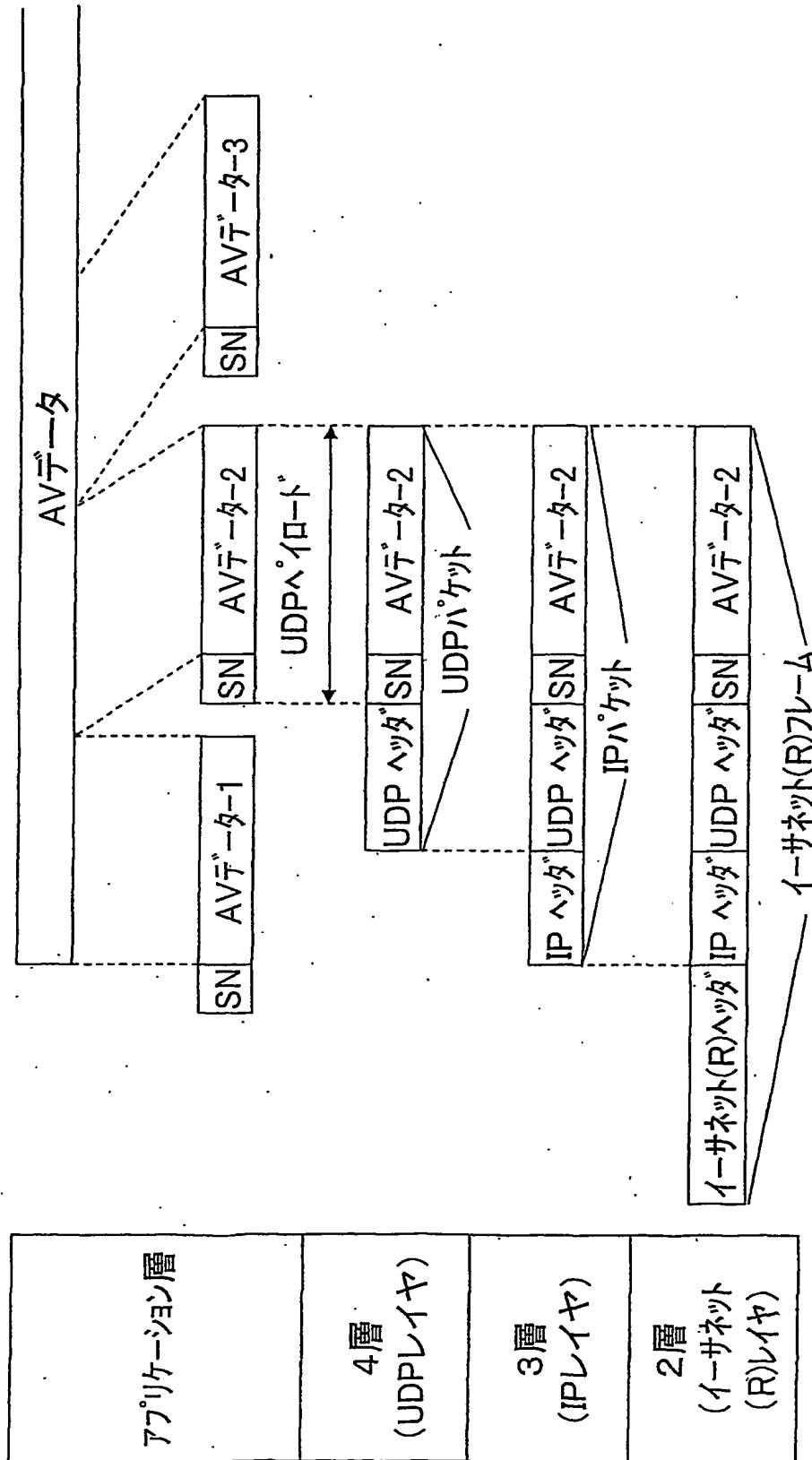
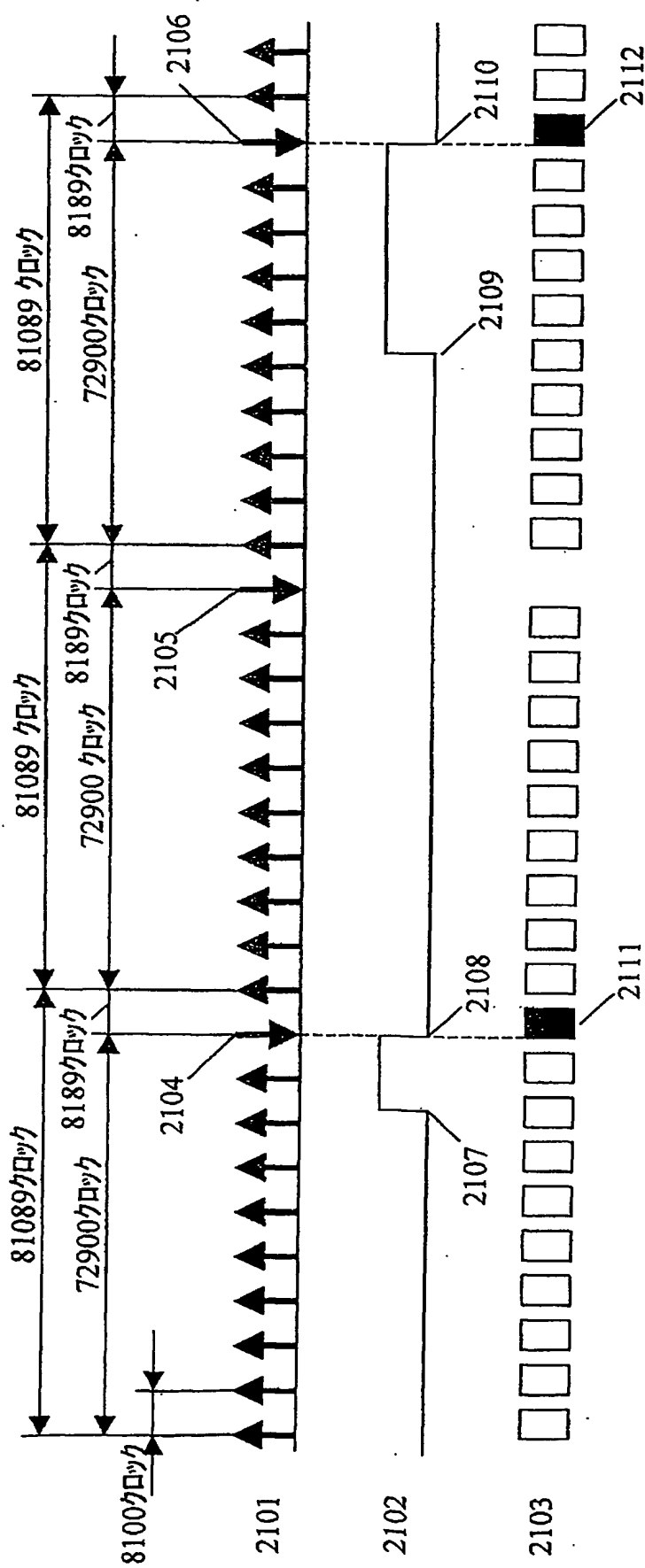


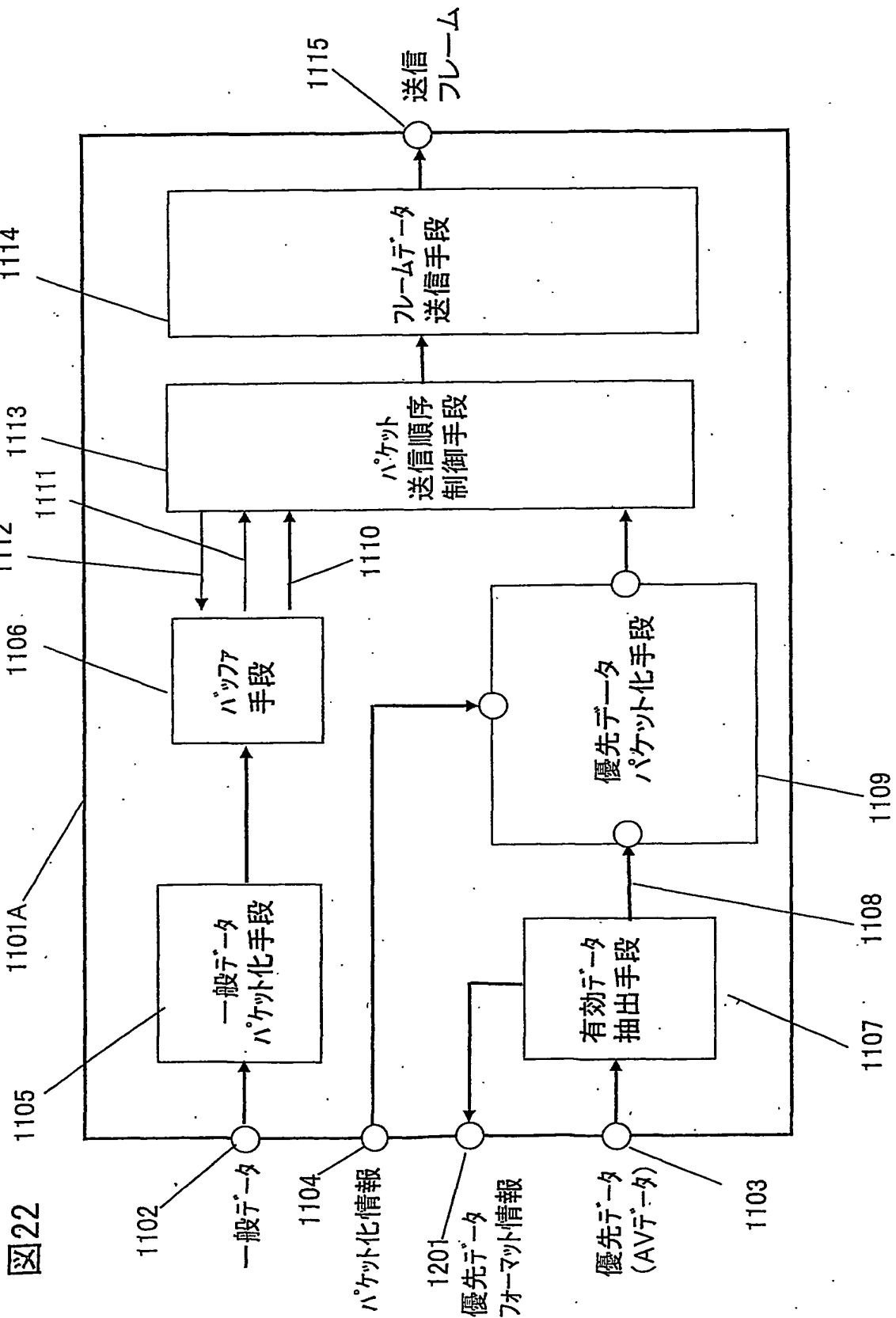
図20

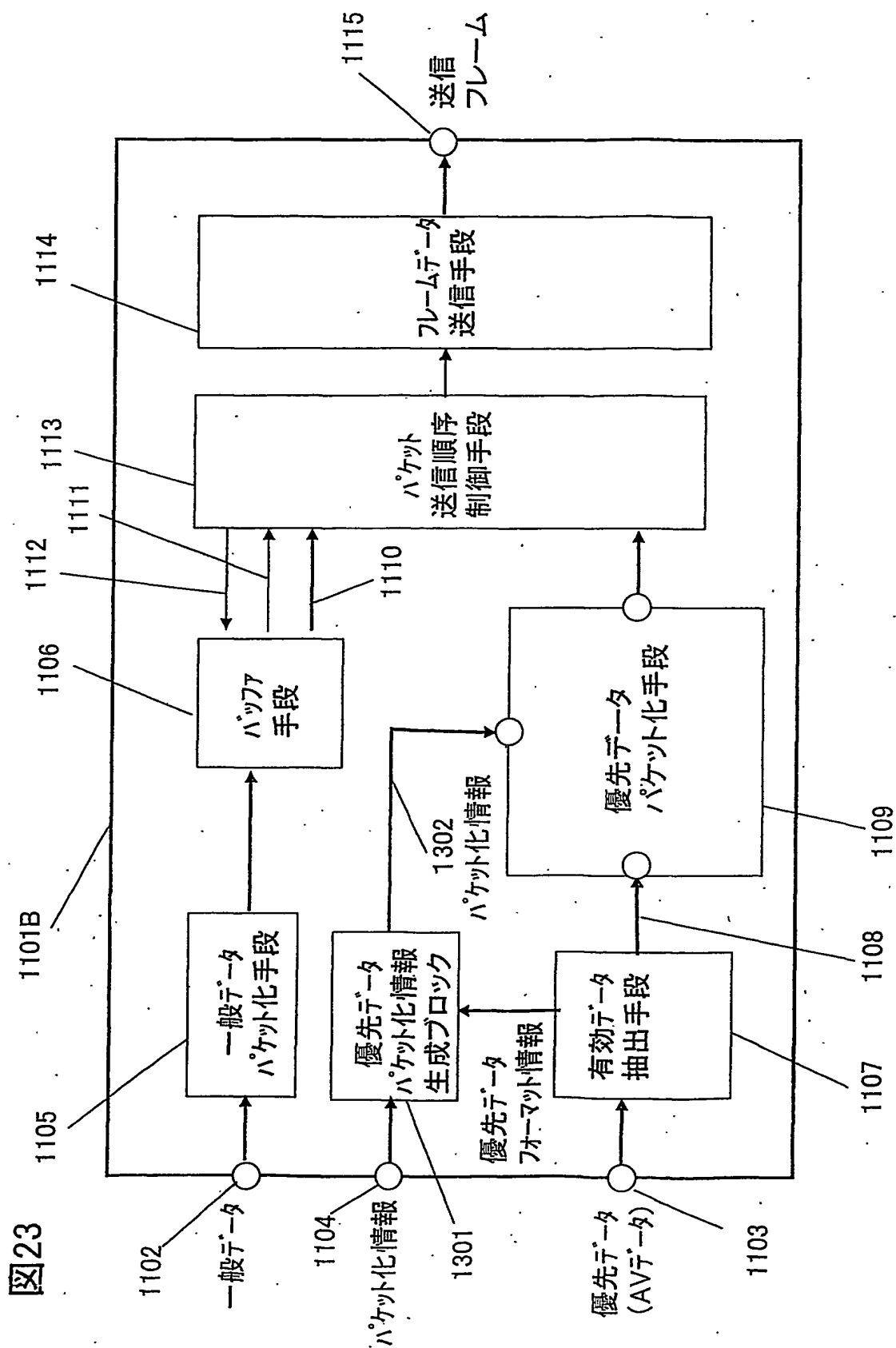


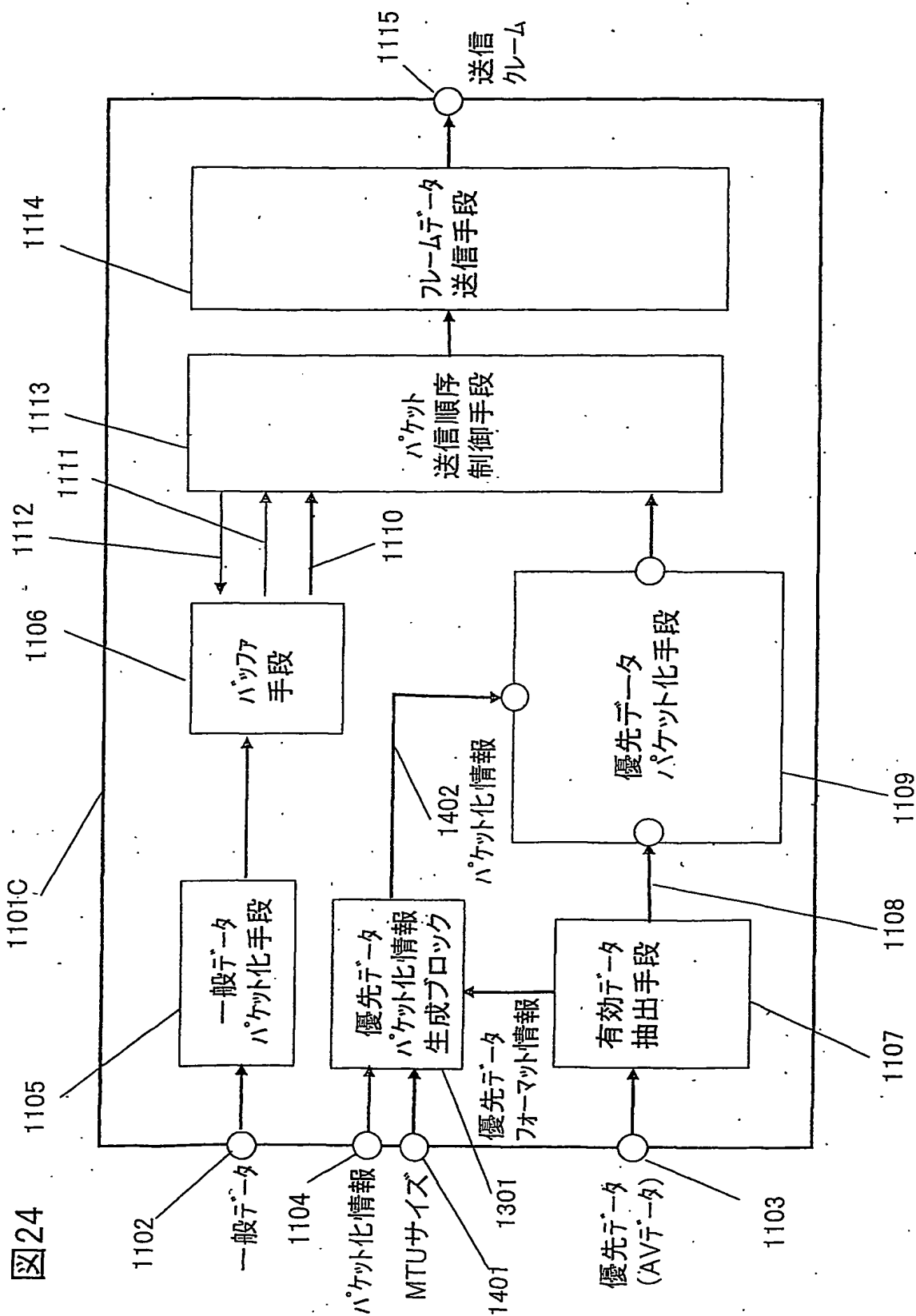
(OSIモデルによる表現)

図21









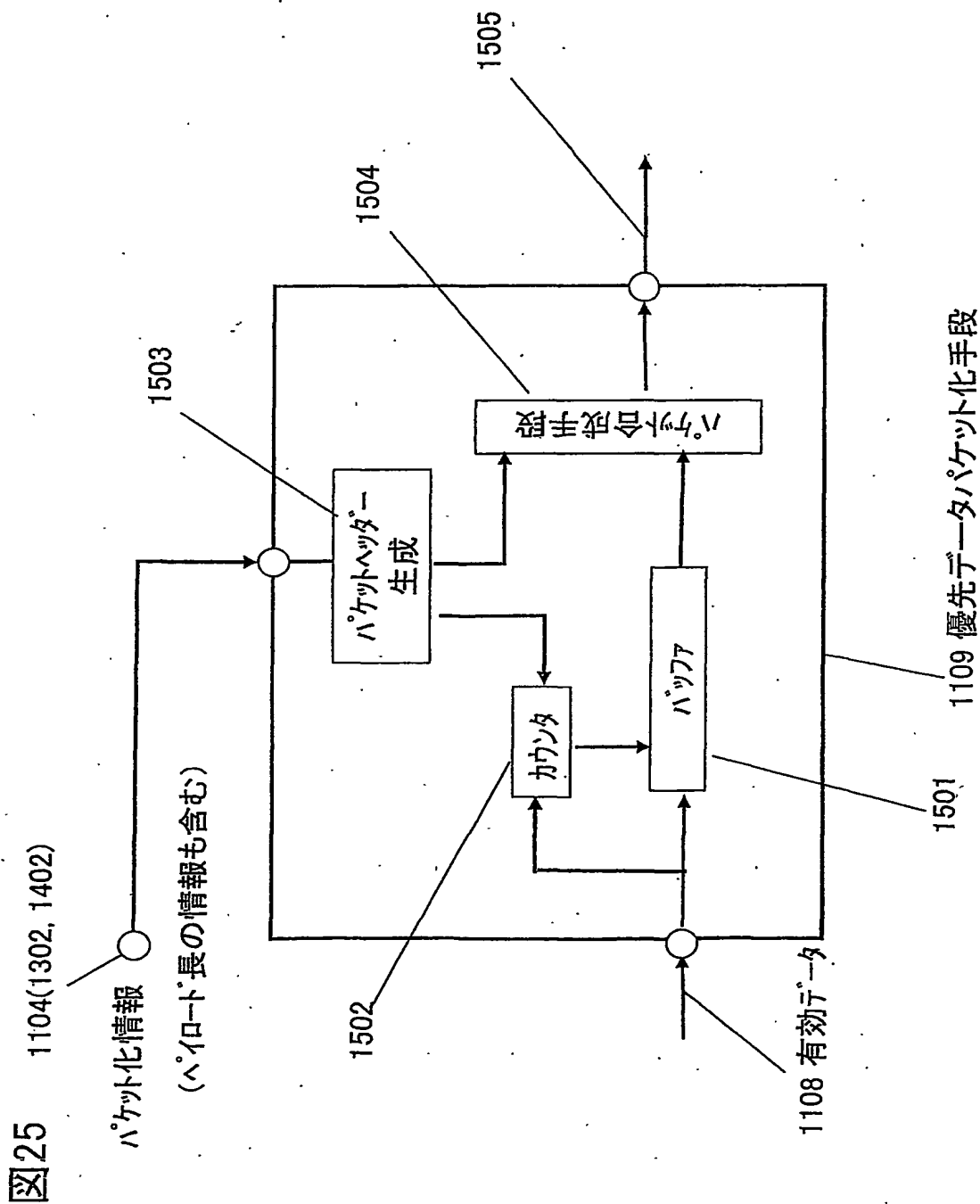
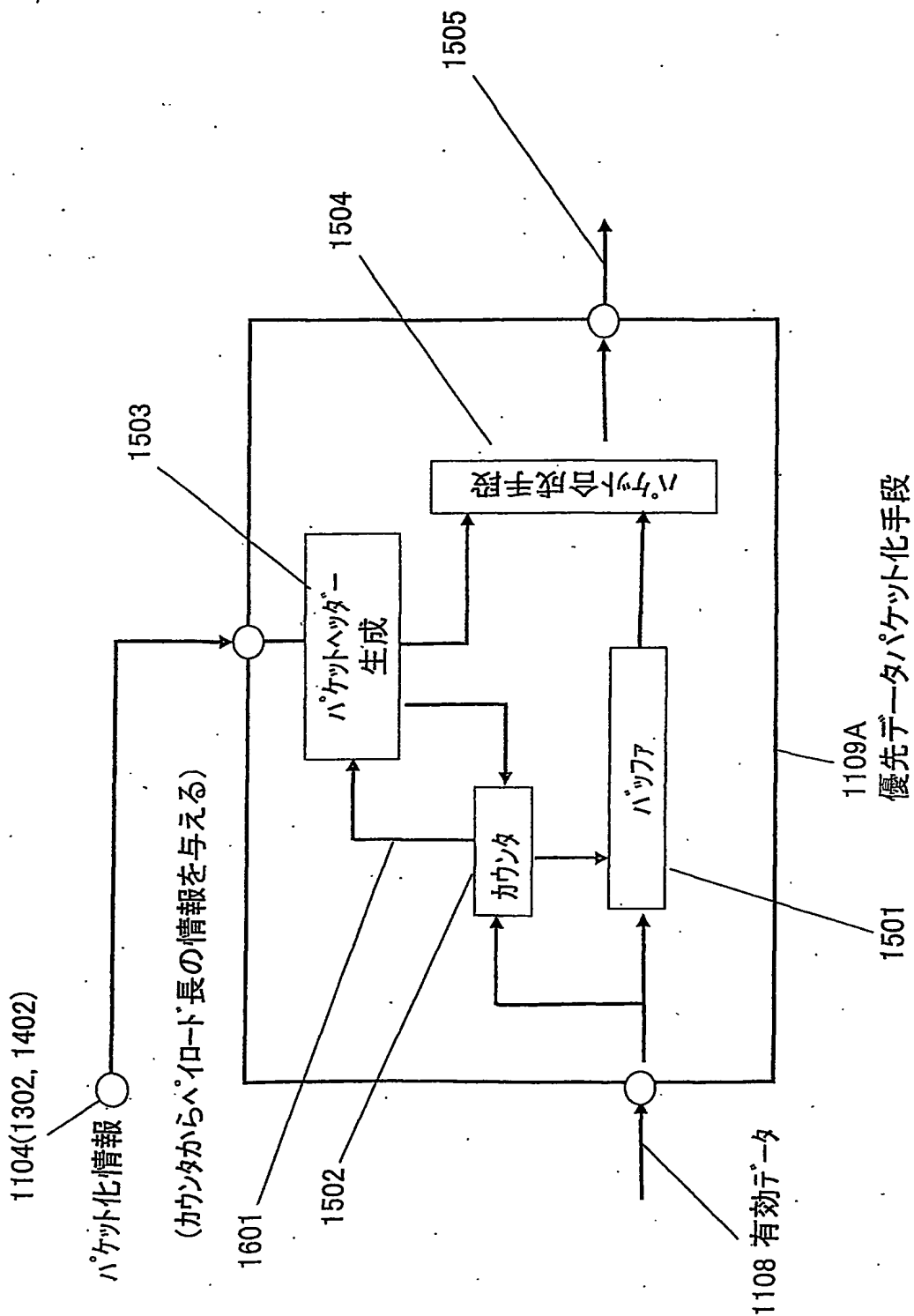


図26



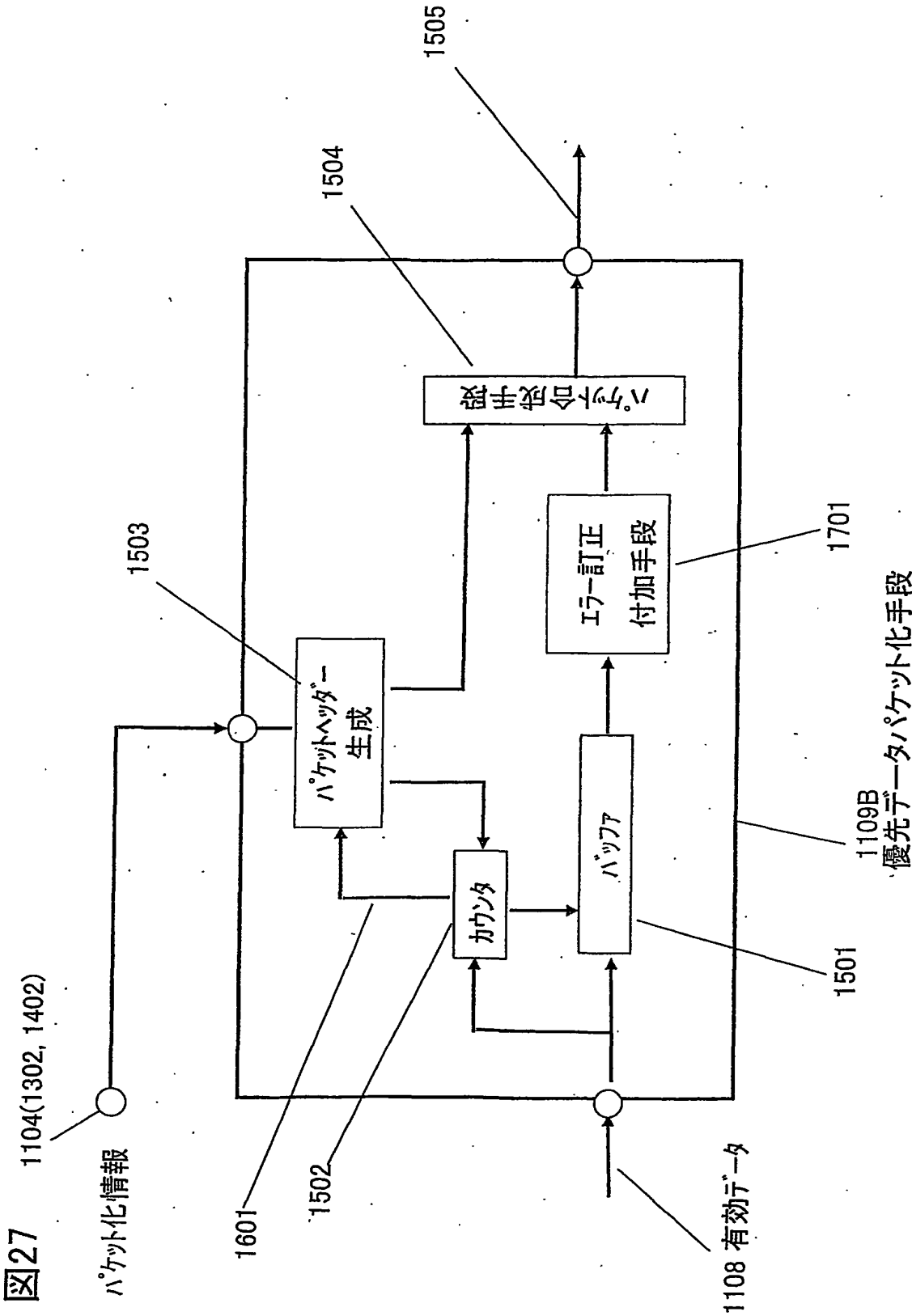
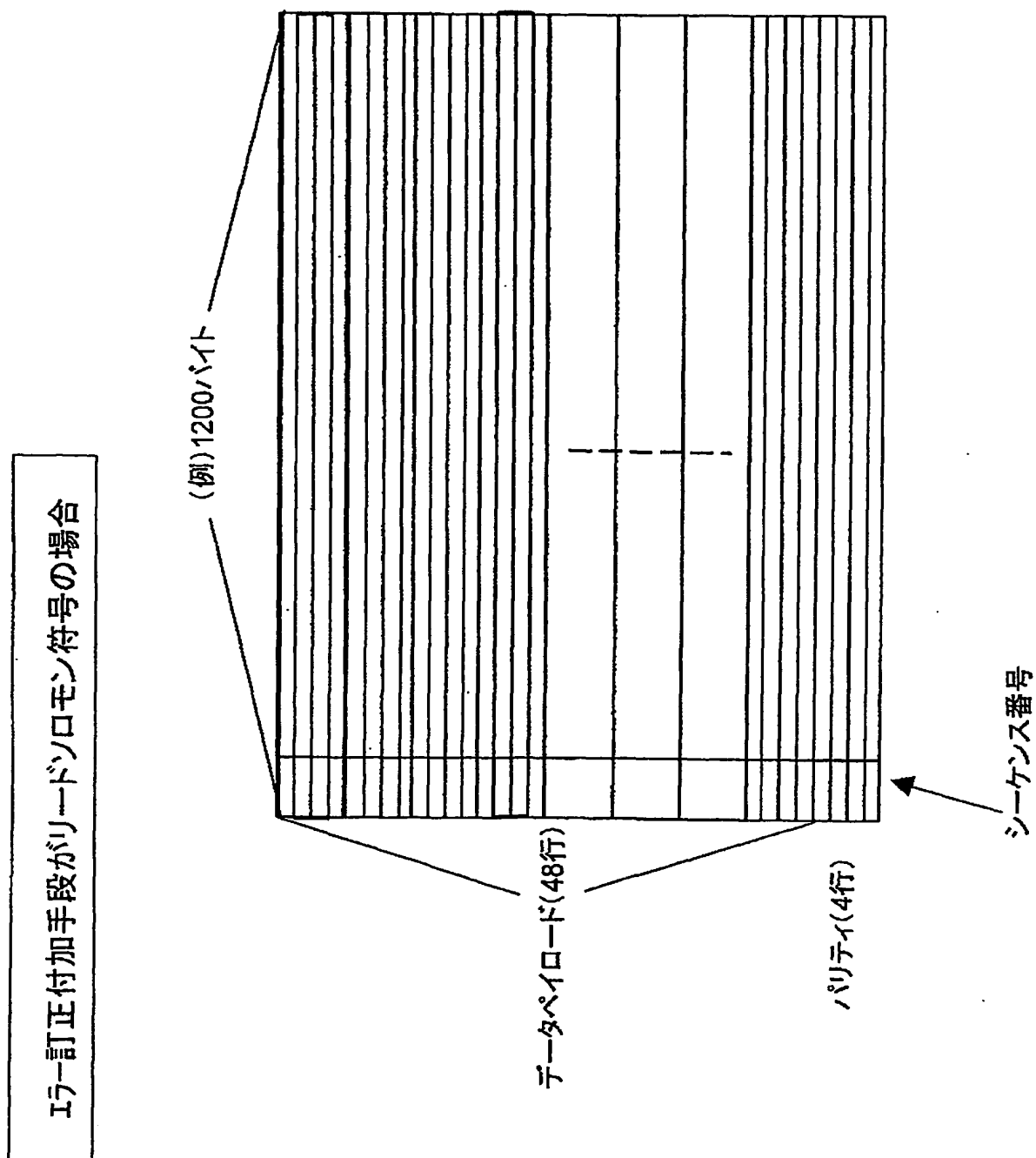
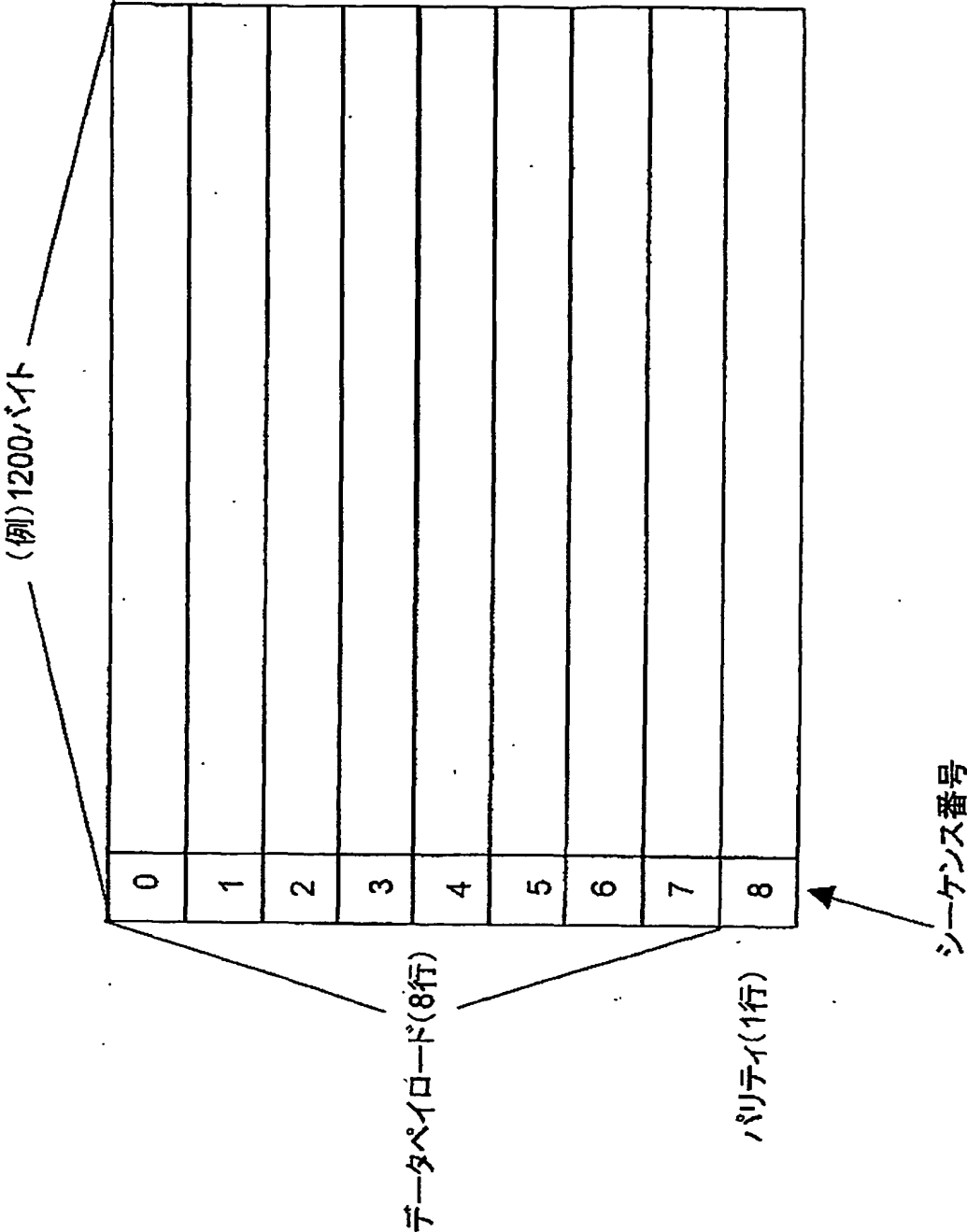


図28



エラー訂正付加手段がパリティの場合

図29



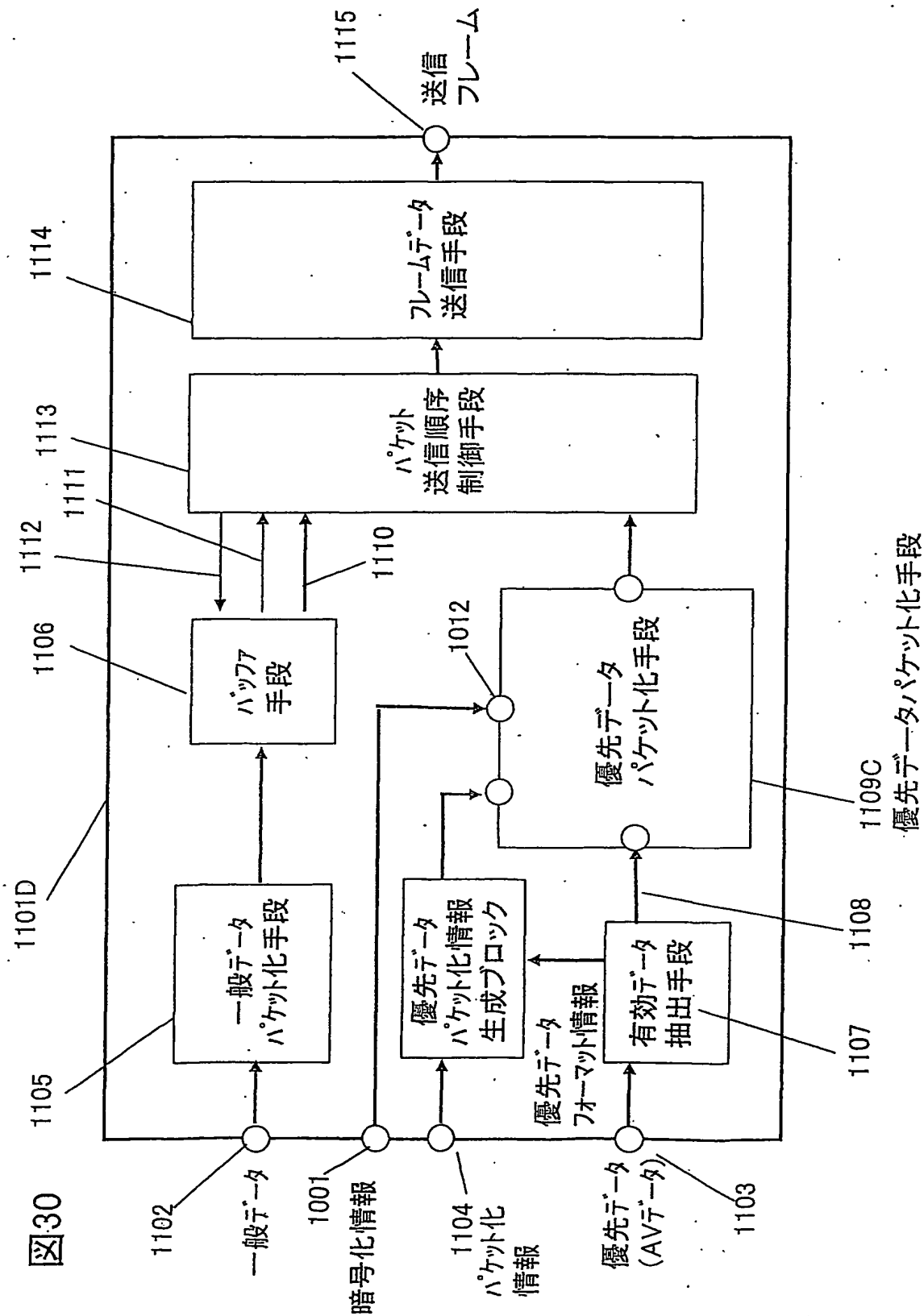
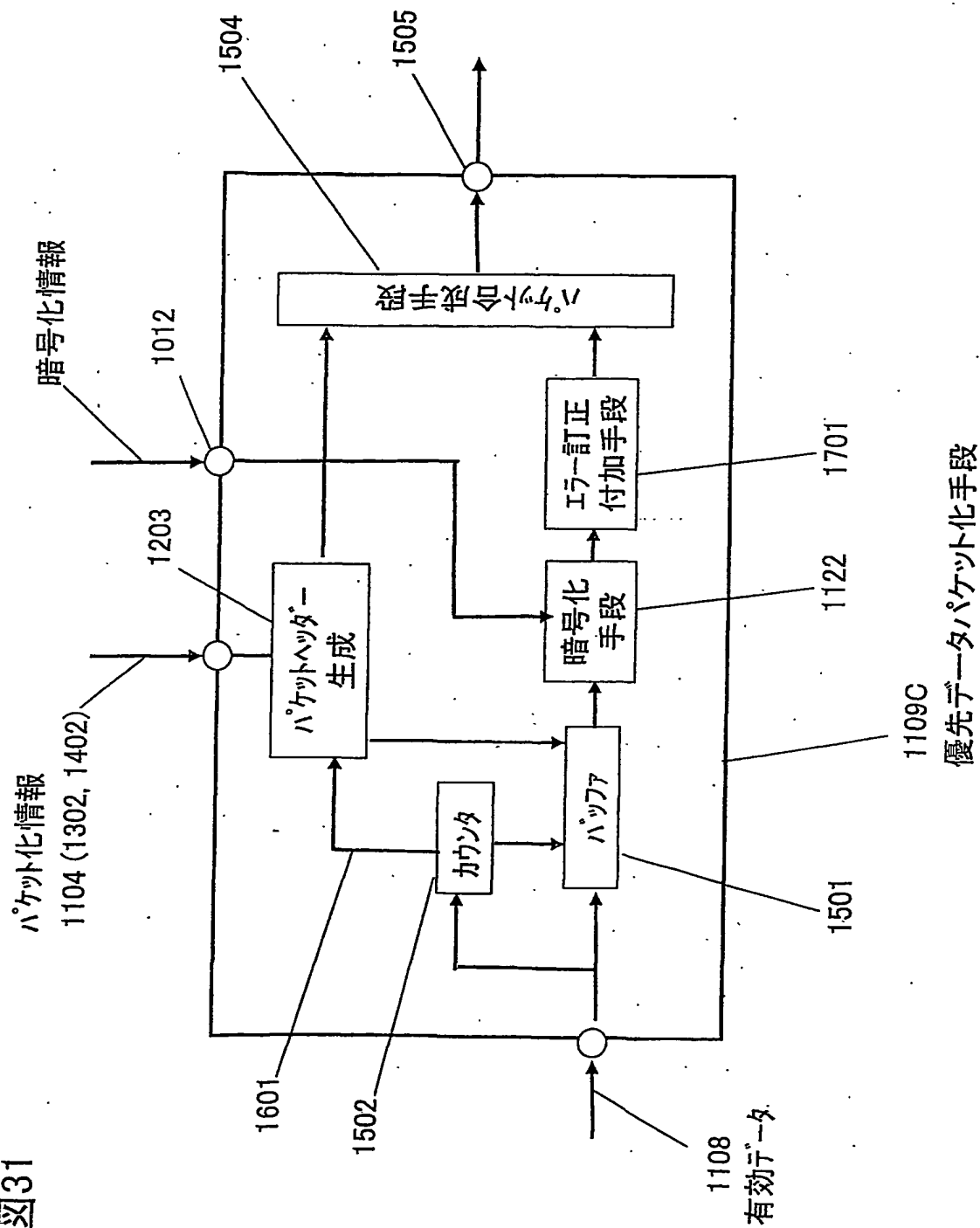


図31



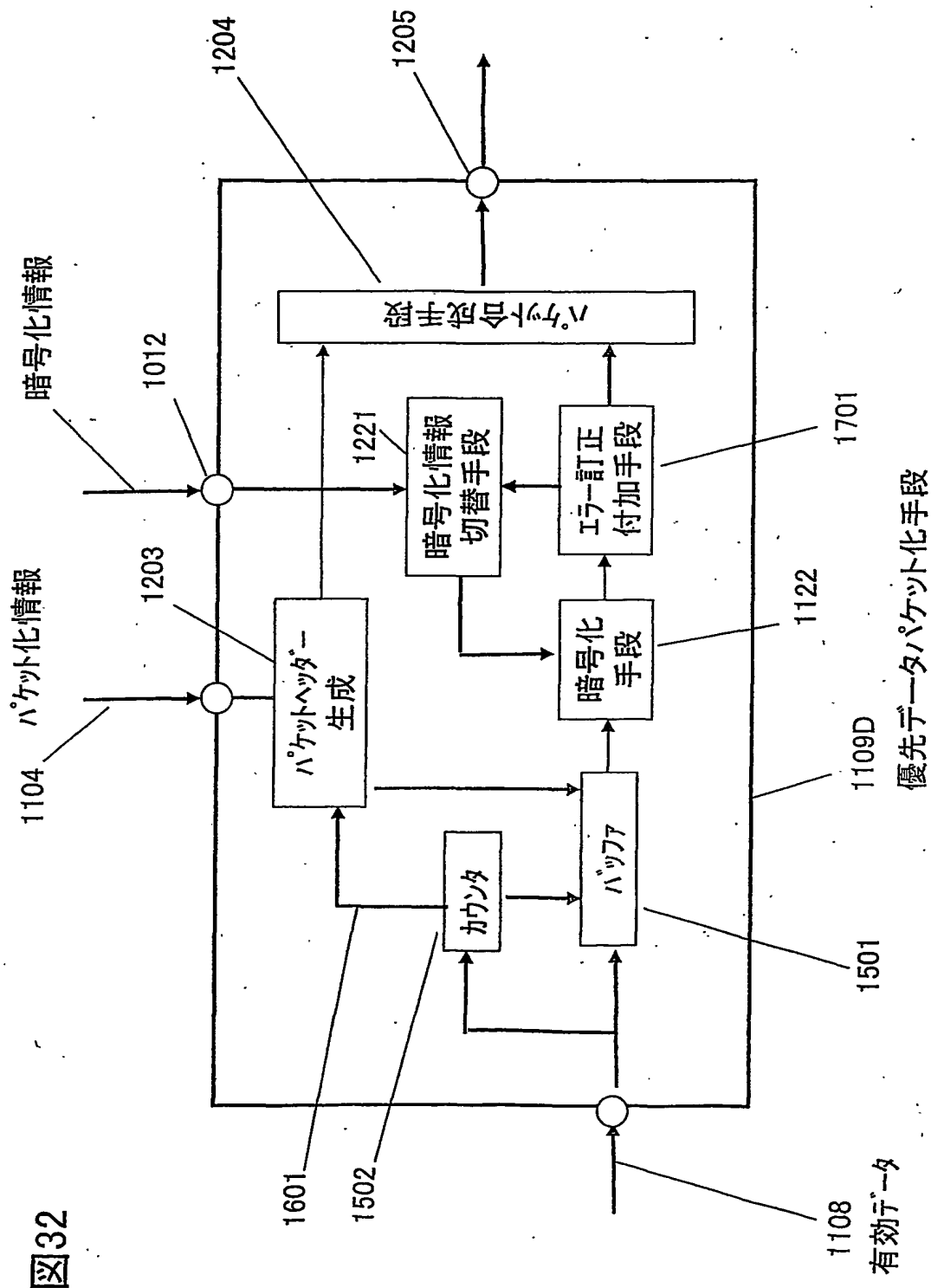
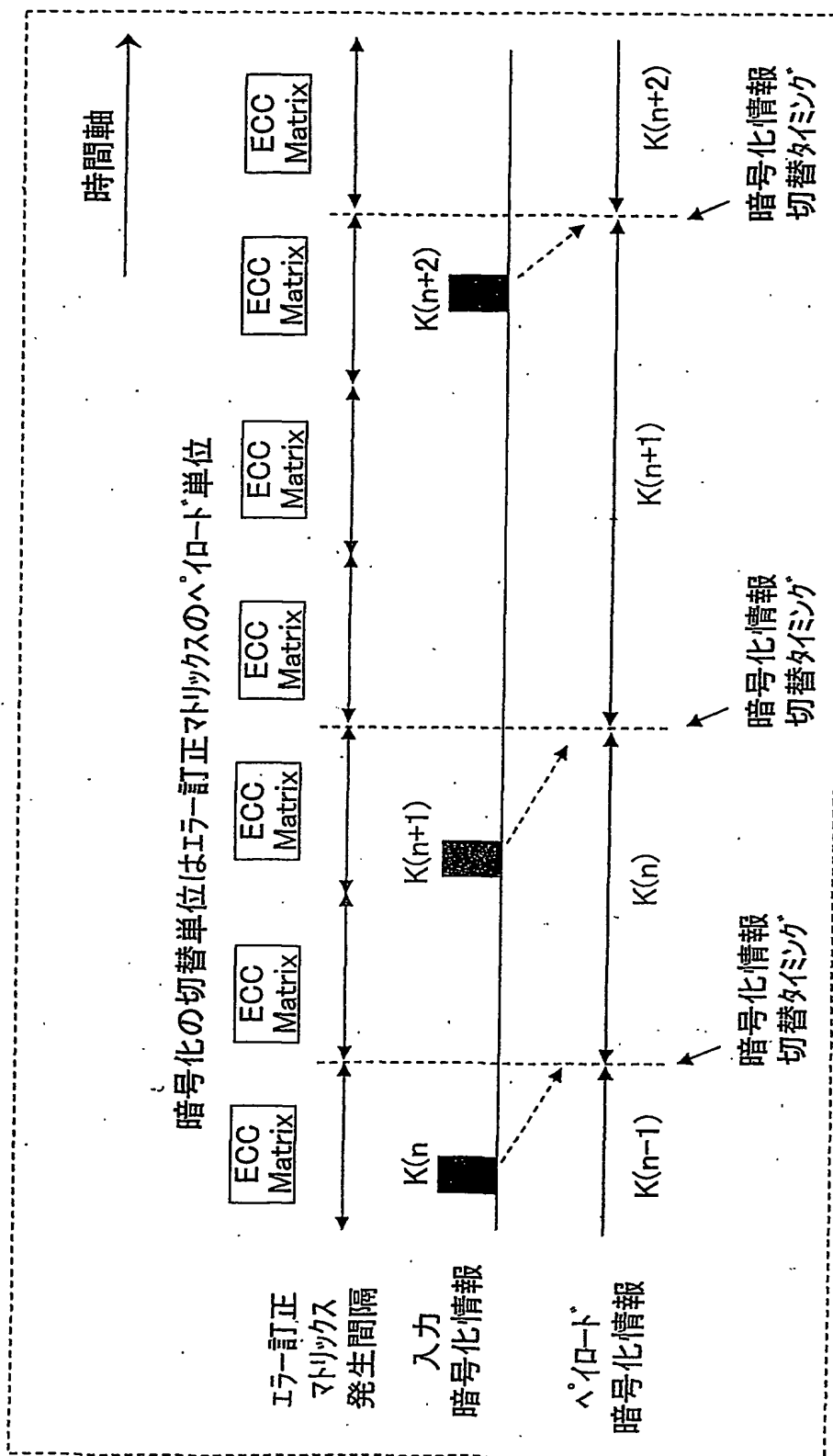
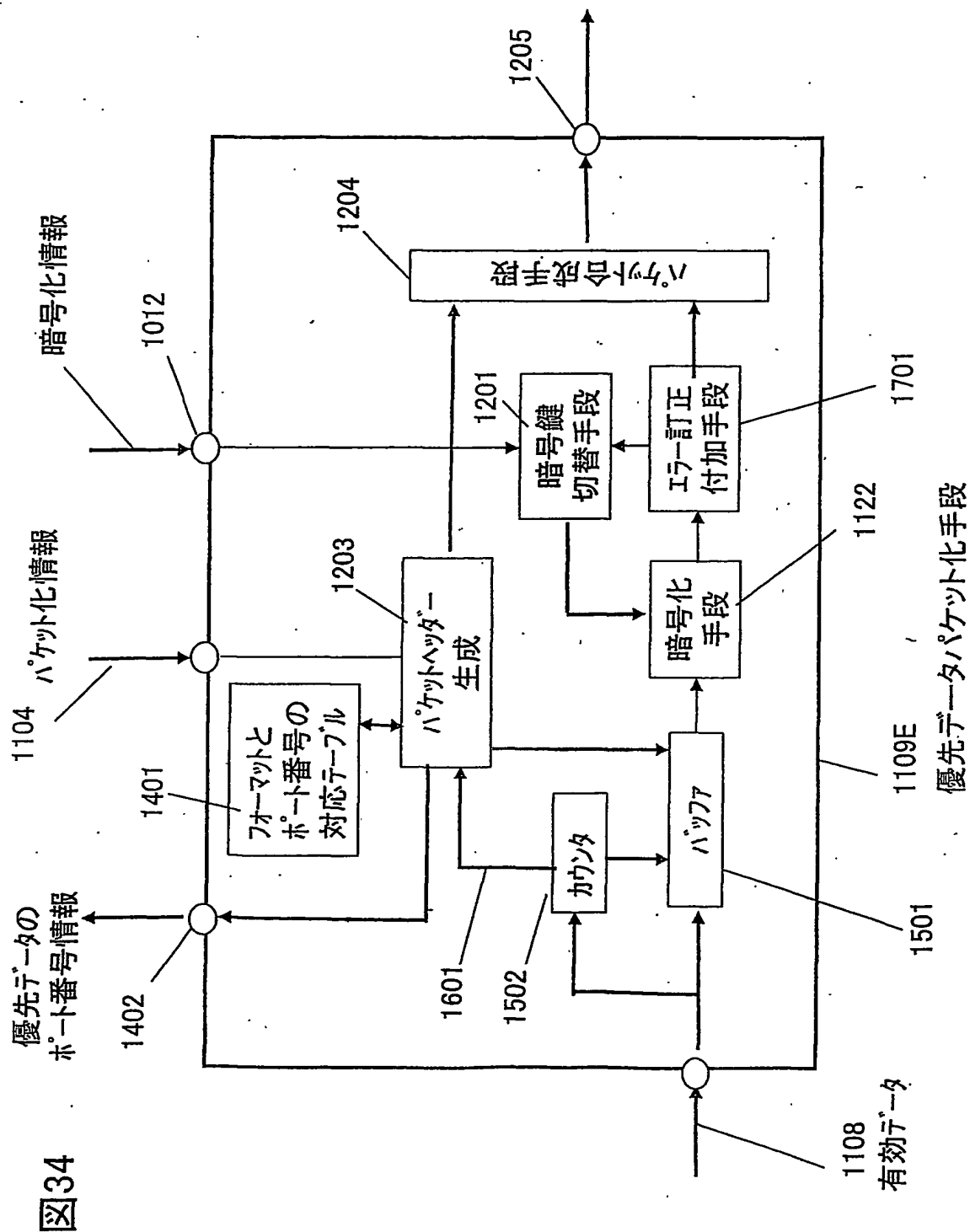
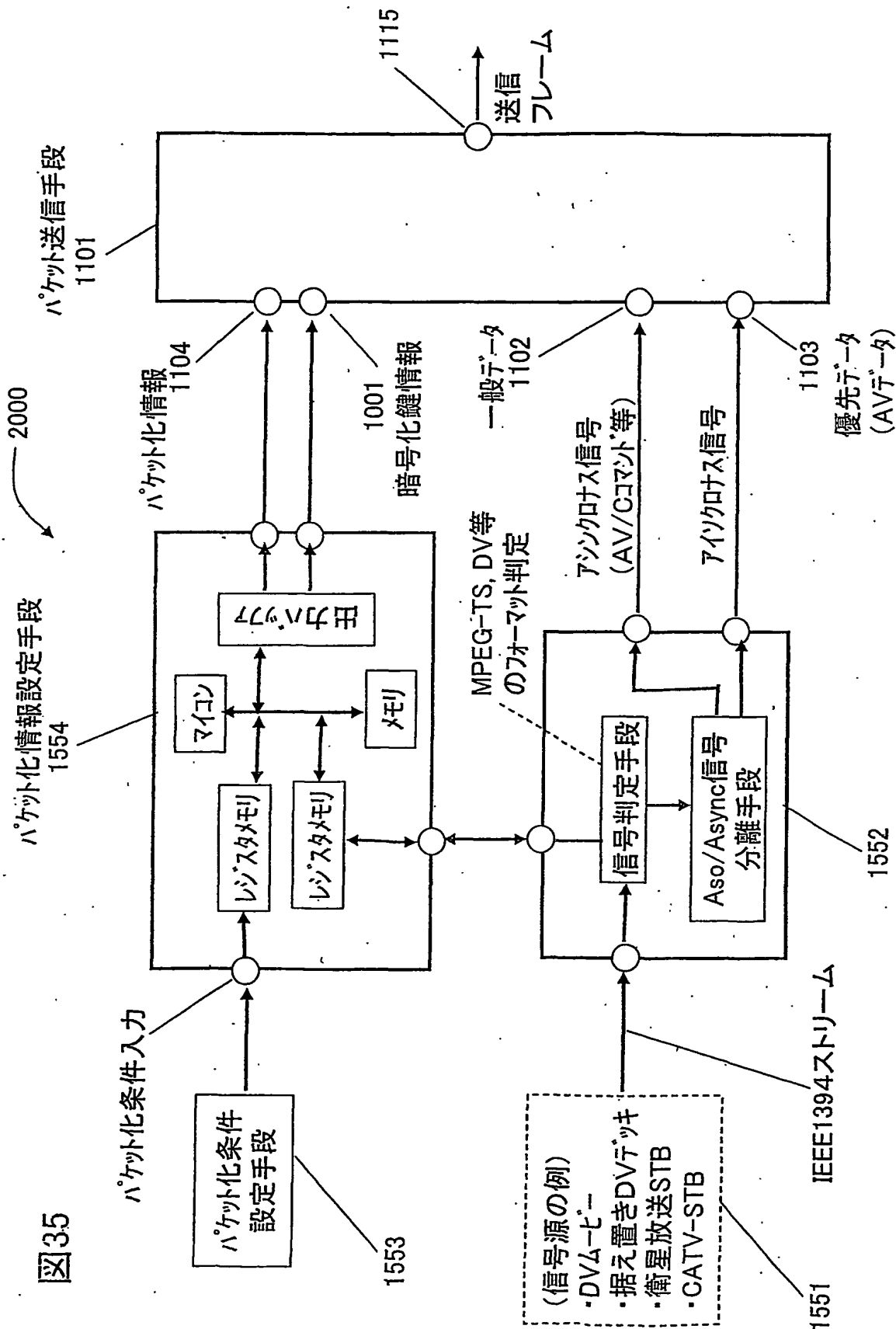
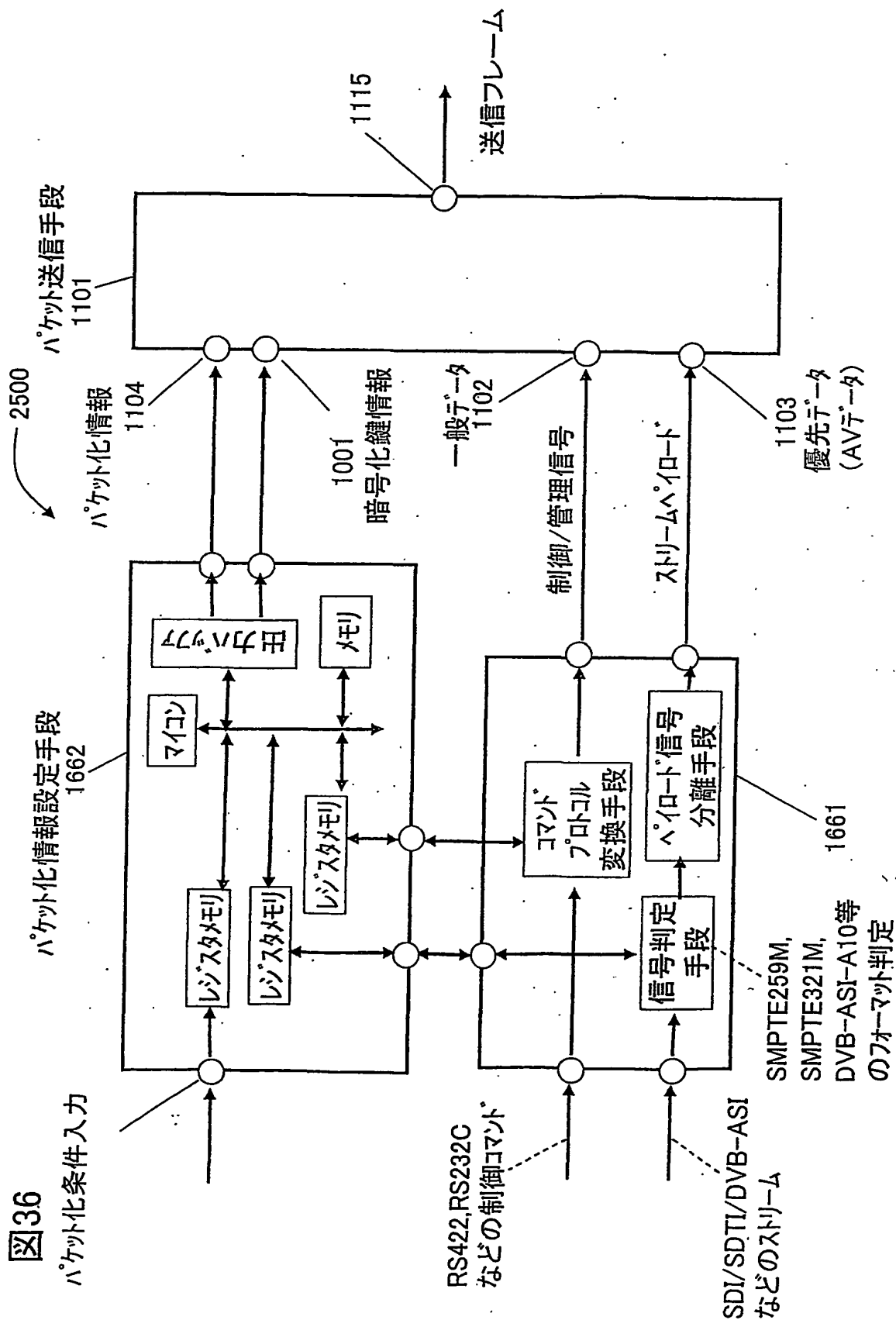


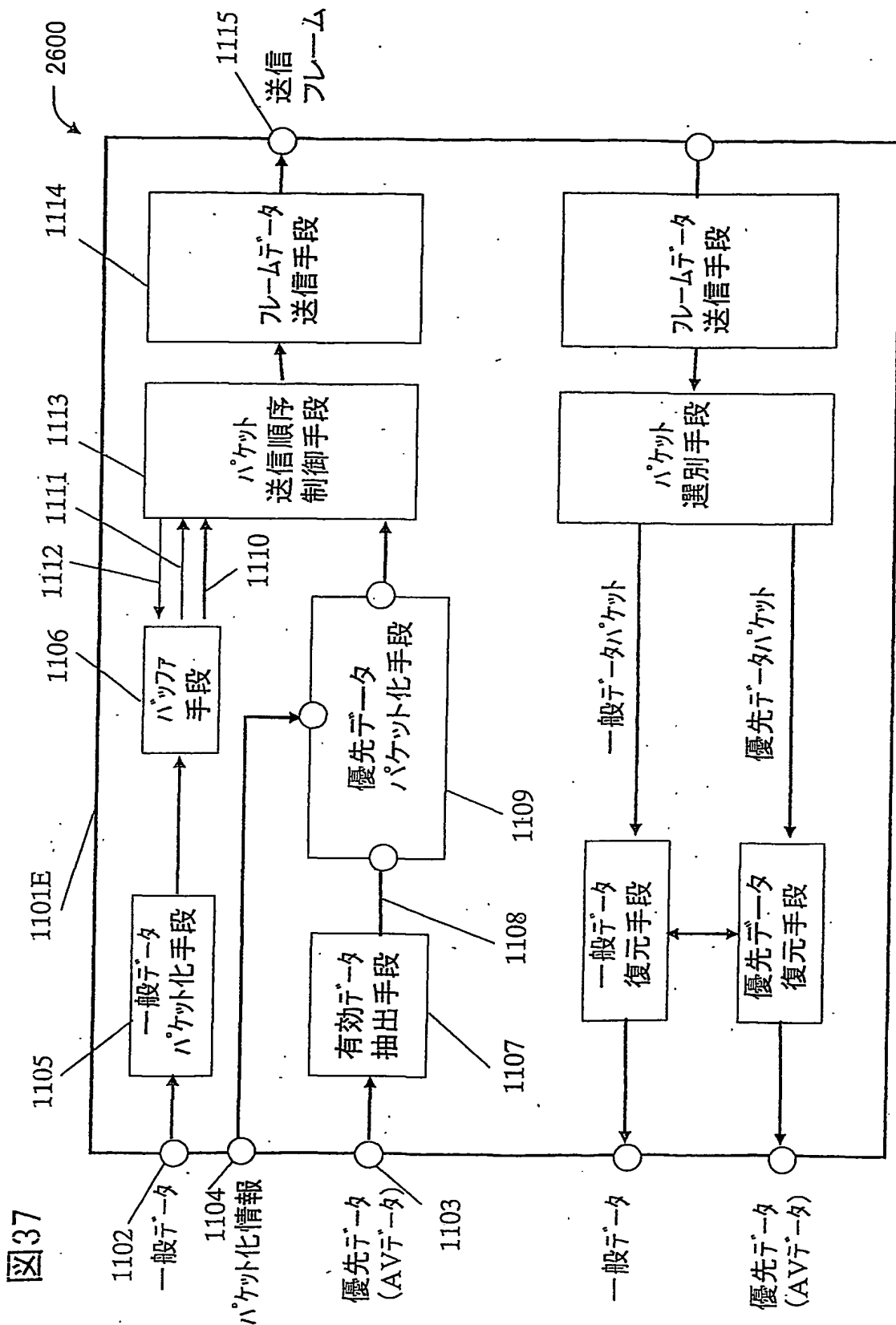
図33

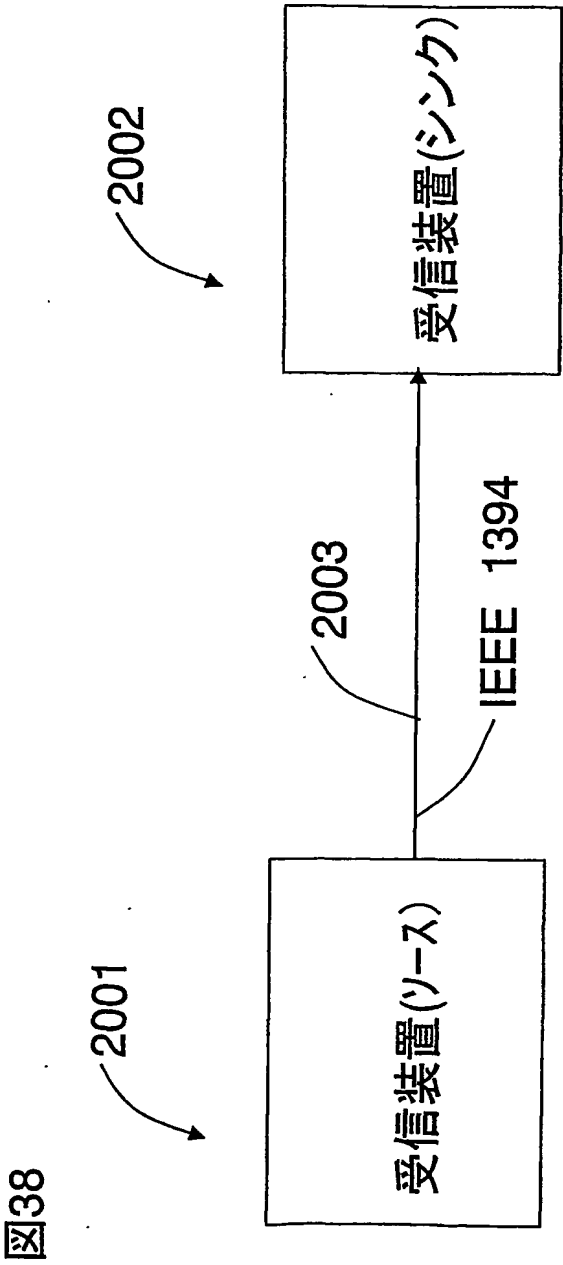












INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/13218A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L12/56, H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L12/56, H04L9/00Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2002-202720 A (Toshiba Corp.), 19 July, 2002 (19.07.02), Abstract & EP 1220079 A2 & US 2003/0126458 A1	1-3, 11-13 4-7, 9, 10, 14-24, 26-28, 31-33, 40-46 8, 25, 29, 30, 34-39, 47-51
X Y A	JP 2000-341324 A (NTT Data Corp.), 08 December, 2000 (08.12.00), Par. No. [0002] (Family: none)	1-3, 11-13 4-7, 9, 10, 14-24, 26-28, 31-33, 40-46 8, 25, 29, 30, 34-39, 47-51

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
---	--

Date of the actual completion of the international search
04 December, 2003 (04.12.03)Date of mailing of the international search report
16 December, 2003 (16.12.03)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/13218

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2000-299686 A (NEC Corp.), 24 October, 2000 (24.10.00), Abstract (Family: none)	4-7, 9, 16-24, 40-45 8
Y	JP 2002-217961 A (Fujitsu Ltd.), 02 August, 2002 (02.08.02), Claim 2 & US 2002/0097733 A1	9
Y	Michiya TAKADA, Yoshihisa MIWA, "Tokushu 2 Internet no Kiban 'IP o Shiru'", Nikkei Network, Nikkei Business Publications, Inc., No.30, 22 September, 2002 (22.09.02), pages 124 to 139; "Yakuwari 3 Packet o Bunkatsu Suru Toru Kaisen ni Awasete Okisa o Chosei" (pages 132 to 135)	10, 42-45
Y	JP 2001-186173 A (Matsushita Electric Industrial Co., Ltd.), 06 July, 2001 (06.07.01), Par. No. [0153] & US 6636481 B1 & CN 1264233 A	14, 15
Y	Michiya TAKADA, "Internet ni yoru Anzen na LAN-kan Tsushin VPN o Oku made Saguru", Nikkei Network, Nikkei Business Publications, Inc., No.25, 22 April, 2002 (22.04.02), pages 51 to 69; Figs. 2 to 4 (page 65)	16-24, 40-45
Y	JP 2002-26906 A (Mitsubishi Electric Corp.), 25 January, 2002 (25.01.02), Par. No. [0037] (Family: none)	18-21, 40-45
Y	JP 2002-232955 A (Denso Corp.), 16 August, 2002 (16.08.02), Claims 1 to 3 (Family: none)	26-28, 31, 32
Y A	JP 11-196081 A (Kabushiki Kaisha Kodo Ido Tsushin Security Gijutsu Kenkyusho), 21 July, 1999 (21.07.99), Par. No. [0003] (Family: none)	33, 46 34-39, 47-51
Y	JP 7-297831 A (Sumitomo Electric Industries, Ltd.), 10 November, 1995 (10.11.95), Par. No. [0038] (Family: none)	41

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. C17 H04L12/56, H04L 9/00

B. 調査を行った分野
調査を行った最小限資料 (国際特許分類 (IPC))
Int. C17 H04L12/56, H04L 9/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
日本国公開実用新案公報 1971-2003年
日本国登録実用新案公報 1994-2003年
日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y A	JP 2002-202720 A (株式会社東芝) 2002.07.19 要約 &EP 1220079 A2 &US 2003/0126458 A1	1-3, 11-13 4-7, 9, 10, 14- 24, 26-28, 31- 33, 40-46 8, 25, 29, 30, 34-39, 47-51

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日
04.12.03

国際調査報告の発送日

16.12.03

国際調査機関の名称及びあて先
日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)
石井 研一

5X 3047

電話番号 03-3581-1101 内線 3596

C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y A	J P 2000-341324 A (株式会社エヌ・ティ・ティ・ データ) 2000. 12. 08 第0002段落 (ファミリーなし)	1-3, 11-13 4-7, 9, 10, 14- 24, 26-28, 31- 33, 40-46 8, 25, 29, 30, 34-39, 47-51
Y A	J P 2000-299686 A (日本電気株式会社) 2000. 10. 24 要約 (ファミリーなし)	4-7, 9, 16-24, 40-45, 8
Y	J P 2002-217961 A (富士通株式会社) 2002. 08. 02 請求項2 &US 2002/0097733 A1	9.
Y	高田 学也, 三輪 芳久, “特集2 インターネットの基盤 「I Pを知る」”, 日経ネットワーク, 日経BP社, 第30号, 2002. 09. 22, pp.124-139 “役割3 パケットを分割する 通る回線に合わせて大きさを 調整” (pp.132-135)	10, 42-45
Y	J P 2001-186173 A (松下電器産業株式会社) 2001. 07. 06 第0153段落 &US 6636481 B1 &CN 1264233 A	14, 15
Y	高田 学也, “インターネットによる安全なLAN間通信 VPN を奥まで探る”, 日経ネットワーク, 日経BP社, 第25号, 2002. 04. 22, pp.51-69 第2-4図 (p.65)	16-24, 40-45
Y	J P 2002-26906 A (三菱電機株式会社) 2002. 01. 25 第0037段落 (ファミリーなし)	18-21, 40-45
Y	J P 2002-232955 A (株式会社デンソー) 2002. 08. 16 請求項1-3 (ファミリーなし)	26-28, 31, 32

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	J P 11-196081 A (株式会社高度移動通信 セキュリティ技術研究所) 1999. 07. 21 第0003段落 (ファミリーなし)	33, 46 34-39, 47-51
Y	J P 7-297831 A (住友電気工業株式会社) 1995. 11. 10 第0038段落 (ファミリーなし)	41